



S4140, S4212 & S4224



Web User Guide

33558 Rev. B

Trademarks

All trademarks and registered trademarks are the property of their respective owners.

Copyright Notice/Restrictions

Copyright © 2013-2015 Transition Networks. All rights reserved. No part of this work may be reproduced or used in any form or by any means (graphic, electronic or mechanical) without written permission from Transition Networks. The information contained herein is confidential property of Transition Networks, Inc. The use, copying, transfer or disclosure of such information is prohibited except by express written agreement with Transition Networks, Inc.

S4xxx Ethernet Access/Aggregation Switch Web User Guide, 33558 Rev. B

Contact Information

Transition Networks
 10900 Red Circle Drive
 Minnetonka, MN 55343 USA
 Tel: 952-941-7600 or 1-800-526-9267
 Fax: 952-941-2322

Revision History

| Rev | Date | Description |
|-----|----------|---|
| A | 09/20/13 | Initial release. |
| B | 07/20/15 | Updated to v 2.2 which adds GVRP, Service Activation Tests, DDMI, UDLD, PFC, and Perf- Mon support. |

Cautions and Warnings

Definitions

Cautions indicate that there is the possibility of poor equipment performance or potential damage to the equipment. Warnings indicate that there is the possibility of injury to a person. Cautions and Warnings appear here and may appear throughout this manual where appropriate. Failure to read and understand the information identified by these symbols could result in poor equipment performance, damage to the equipment, or injury to persons. See the related Install Guide manual for specific Cautions and Warnings.

These products are not intended for use in life support products where failure of a product could reasonably be expected to result in death or personal injury. Anyone using this product in such an application without express written consent of an officer of Transition Networks does so at their own risk, and agrees to fully indemnify Transition Networks for any damages that may result from such use or sale.

Table of Contents

| | |
|---|-----------|
| 1. Introduction | 12 |
| Document Overview | 12 |
| Related Manuals and Online Help | 13 |
| 2. Web Interface Menu System | 14 |
| Configuration Main Menu | 16 |
| Configuration > System | 16 |
| Character Support Note | 17 |
| IP Configuration | 18 |
| NTP Configuration | 23 |
| Time Configuration | 24 |
| Time Zones List | 26 |
| Log (System Log) Configuration | 27 |
| Ports Configuration | 29 |
| Configuration > Ports > Shared Port Configuration | 29 |
| Configuration > Ports > Configuration | 30 |
| DHCP Configuration | 33 |
| Configuration > DHCP | 33 |
| Configuration > DHCP > DHCP Server | 33 |
| Global Mode | 34 |
| VLAN Mode | 34 |
| Pool Setting | 36 |
| Configuration > DHCP > DHCP Snooping | 41 |
| Configuration > DHCP > DHCP Relay | 42 |
| S4224 DHCP Configuration Process | 44 |
| A. At Configuration > System > IP | 44 |
| B. At Configuration > DHCP | 44 |
| Web Interface Screen Examples | 45 |
| Additional Notes | 47 |
| DHCP Options Used | 47 |
| System Users Configuration | 49 |
| Configuration > Security > Switch > Users | 49 |
| Edit User (Edit the Default <i>admin</i> User) | 50 |
| Add a New User | 50 |
| Delete an Existing User | 51 |
| Privilege Level Configuration | 52 |
| Configuration -> Security > Switch > Privilege Levels | 52 |
| Authentication Method Configuration | 55 |
| Configuration > Security > Switch > Auth Method | 55 |
| Authentication Method Configuration | 55 |
| Command Authorization Method Configuration | 56 |
| Accounting Method Configuration | 56 |
| SSH Configuration | 59 |
| HTTPS Configuration | 60 |
| Access Management Configuration | 64 |
| SNMP Configuration | 66 |
| SNMP v1 Traps | 70 |
| SNMP v2 Traps | 70 |
| SNMP v3 Traps | 70 |
| SNMP v3 Configuration Process | 70 |
| SNMP System Configuration | 71 |
| SNMP Trap Configuration | 72 |
| SNMP Trap Event | 74 |
| Specific Trap Event Configuration | 75 |
| SNMPv3 Community Configuration | 77 |

| | |
|--|------------|
| SNMPv3 User Configuration..... | 78 |
| SNMPv3 Group Configuration | 80 |
| SNMPv3 Views Configuration..... | 81 |
| SNMPv3 Access Configuration..... | 82 |
| Configuration > Security > Switch > RMON | 84 |
| RMON > Statistics | 84 |
| RMON > History | 85 |
| RMON > Alarm | 87 |
| RMON > Event | 89 |
| Port Security Limit Control Configuration..... | 91 |
| Configuration > Security > Network > Limit Control | 91 |
| System Configuration | 91 |
| Port Configuration | 92 |
| NAS (Network Access Server) Configuration | 94 |
| Configuration > Security > Network > NAS | 94 |
| NAS System Configuration | 95 |
| NAS Port Configuration | 97 |
| ACL Ports Configuration | 102 |
| Access Controls Lists | 102 |
| ACL Rate Limiter Configuration | 105 |
| Access Control List (ACL) Configuration..... | 106 |
| ACE Configuration | 107 |
| ACE Configuration Parameters | 113 |
| MAC Parameters | 113 |
| VLAN Parameters..... | 114 |
| ARP Parameters..... | 114 |
| IPv4 Parameters | 116 |
| IPv6 Parameters | 118 |
| ICMP Parameters | 119 |
| TCP Parameters | 120 |
| UDP Parameters..... | 122 |
| Ethernet Type Parameters..... | 123 |
| Bandwidth Profile using ACE (Access Control Entry)..... | 124 |
| IP Source Guard Configuration | 125 |
| IP Source Guard > Configuration | 126 |
| Port Mode Configuration | 126 |
| IP Source Guard > Static Table | 127 |
| ARP Inspection Configuration | 129 |
| Port Configuration..... | 129 |
| VLAN Configuration | 131 |
| VLAN Mode Configuration..... | 131 |
| Static ARP Inspection | 132 |
| Dynamic ARP Inspection | 134 |
| AAA Security Configuration..... | 136 |
| Config > Security > AAA > RADIUS | 137 |
| Global Configuration | 137 |
| Server Configuration..... | 138 |
| Config > Security > AAA > TACACS+ | 139 |
| Global Configuration | 139 |
| Server Configuration..... | 139 |
| Adding a New Server..... | 140 |
| Aggregation Configuration | 141 |
| Static Aggregation | 142 |
| Aggregation Mode Configuration - Hash Code Contributors | 143 |
| Aggregation Group Configuration | 143 |
| LACP (Link Aggregation Control Protocol) | 145 |

| | |
|--|------------|
| Link OAM (LOAM) Configuration | 148 |
| Link OAM Port Settings | 149 |
| Link OAM Event Settings..... | 151 |
| Detailed Link OAM Status | 153 |
| Loop Protection Configuration | 155 |
| Spanning Tree | 157 |
| STP/RSTP/MSTP | 157 |
| Bridge Settings..... | 158 |
| MSTI Mapping..... | 161 |
| Configuration Identification | 161 |
| MSTI Mapping | 161 |
| MSTI Priorities | 163 |
| CIST Ports | 164 |
| MSTI Ports..... | 167 |
| IPMC Profile Configuration | 169 |
| > Profile Table..... | 170 |
| > Address Entry | 172 |
| Buttons..... | 172 |
| MVR Configuration | 175 |
| VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver]) | 175 |
| IPMC (IP MultiCast) | 178 |
| IGMP Snooping..... | 179 |
| Basic Configuration | 179 |
| VLAN Configuration..... | 182 |
| IGMP Snooping VLAN Table Columns | 182 |
| Port Filtering Profile | 185 |
| MLD Snooping | 186 |
| Basic Configuration | 186 |
| VLAN Configuration..... | 189 |
| Port Filtering Profile | 192 |
| L2CP Configuration | 193 |
| LLDP Configuration | 194 |
| LLDP Configuration | 194 |
| LLDP Parameters..... | 195 |
| LLDP Interface Configuration..... | 195 |
| LLDP-MED Configuration | 197 |
| Fast Start Repeat Count..... | 197 |
| Transmit TLVs | 198 |
| Coordinates Location | 198 |
| Civic Address Location..... | 199 |
| Emergency Call Service | 201 |
| Policies | 201 |
| Adding a New Policy..... | 203 |
| Policy Interface Configuration | 203 |
| EPS Configuration | 204 |
| EPS Configuration | 206 |
| EPS Instance Data | 206 |
| EPS Instance Configuration | 207 |
| EPS (Port Protection) Parameter Summary..... | 211 |
| MEP Configuration | 213 |
| Configuration > MEP > Configuration | 214 |
| MEP Instance Configuration | 218 |
| MEP Instance Data..... | 218 |
| Instance Configuration | 218 |
| Peer MEP Configuration..... | 220 |
| MEP Functional Configuration..... | 221 |

| | |
|---|------------|
| Fault Management..... | 223 |
| Performance Monitoring..... | 231 |
| TLV Configuration..... | 240 |
| TLV Status..... | 240 |
| Link State Tracking..... | 241 |
| Add a New Peer MEP Procedure..... | 242 |
| Add a New MIP Procedure..... | 244 |
| ERPS Configuration..... | 246 |
| ERPS Configuration Page..... | 248 |
| ERPS Instance Data..... | 249 |
| ERPS Instance Configuration..... | 250 |
| RPL Configuration..... | 252 |
| Sub-Ring Configuration..... | 252 |
| ERPS Instance Command..... | 253 |
| ERPS Instance State..... | 253 |
| Ring Protection and MEP Configuration..... | 256 |
| Ring Protection Conditions and Commands..... | 256 |
| ERPS VLAN Configuration..... | 257 |
| Add a New ERPS Protection Group Procedure..... | 258 |
| Delete an Existing ERPS Protection Group Procedure..... | 258 |
| ERPS Parameters Summary..... | 259 |
| MAC Address Table Configuration..... | 260 |
| Aging Configuration..... | 261 |
| MAC Table Learning..... | 261 |
| Static MAC Table Configuration..... | 262 |
| VLAN Translation Configuration..... | 264 |
| Port to Group Mapping..... | 264 |
| VLAN Translation Mapping..... | 266 |
| VLANs Configuration..... | 268 |
| Global VLAN Configuration..... | 268 |
| Port VLAN Configuration..... | 269 |
| Provider Bridging (IEEE 802.1ad 2005)..... | 272 |
| Provider Tagging Use cases..... | 272 |
| Private VLANs Configuration..... | 274 |
| PVLAN Membership..... | 274 |
| Port Isolation..... | 276 |
| VCL (VLAN Control List)..... | 277 |
| MAC-based VLAN..... | 277 |
| Protocol-based VLAN..... | 279 |
| Protocol to Group..... | 279 |
| Group to VLAN..... | 282 |
| IP Subnet-based VLAN..... | 284 |
| Ethernet Services Configuration..... | 286 |
| Configuration > Ethernet Services..... | 286 |
| Configuration > Ethernet Services > Ports..... | 287 |
| Configuration > Ethernet Services > Bandwidth Profiles..... | 288 |
| Configuration > Ethernet Services > EVCs..... | 291 |
| Configuration Prerequisites..... | 292 |
| Configuration > Ethernet Services > EVCs..... | 292 |
| Configuration > Ethernet Services > ECEs..... | 294 |
| ECE Configuration Page..... | 298 |
| Ethernet Services Application Example..... | 304 |
| Performance Monitor Configuration..... | 309 |
| PM Session and Storage Configuration..... | 309 |
| PM Transfer Configuration..... | 310 |

| | |
|---|------------|
| QoS Configuration | 312 |
| Bandwidth Profiling | 312 |
| Port Classification | 314 |
| Port Policing..... | 317 |
| Queue Policing..... | 318 |
| Port Scheduler | 320 |
| Scheduler Mode (Strict Priority or Weighted) | 320 |
| Port Shaping | 324 |
| Port Tag Remarking..... | 325 |
| Port DSCP | 328 |
| DSCP-Based QoS | 330 |
| DSCP Translation | 332 |
| DSCP Classification..... | 334 |
| QoS Control List (QCL)..... | 335 |
| Storm Policing..... | 342 |
| WRED (Weighted Random Early Detection) Configuration | 344 |
| RED Drop Probability Function | 345 |
| Mirroring & Remote Mirroring Configuration | 346 |
| Mirroring & Remote Mirroring Configuration..... | 347 |
| Source VLAN(s) Configuration | 347 |
| Port Configuration (Remote Mirroring) | 347 |
| Configuration Guideline for All Features | 348 |
| PTP Clock Configuration..... | 350 |
| External I/O Configuration | 351 |
| Extrenal I/O Options | 351 |
| PTP Clock Configuration | 352 |
| PTP Clock Configuration | 353 |
| GVRP Configuration | 366 |
| Service Activation Configuration | 368 |
| Service Activation Configuration..... | 368 |
| Configuration > Service Activation > System | 368 |
| Configuration > Service Activation > Profiles | 369 |
| Buttons | 372 |
| Configuration > Service Activation > Tests | 373 |
| DDMI Configuration | 376 |
| Configuration > DDMI > General..... | 376 |
| Configuration > DDMI > Thresholds..... | 376 |
| UDLD Configuration..... | 378 |
| Monitor Main Menu | 380 |
| Monitor > System > Information..... | 380 |
| Monitor > System > CPU Load | 382 |
| Monitor > System > IP Status | 385 |
| Monitor > System > Log..... | 387 |
| Detailed System Log Information | 389 |
| System Log Message Summary | 389 |
| Monitor > Ports > State | 390 |
| Detailed Port Statistics | 391 |
| Monitor > Ports > Traffic Overview | 392 |
| Monitor > Ports > QoS Statistics..... | 394 |
| Monitor > Ports > QCL Status..... | 396 |
| Monitor > Ports > Detailed Statistics..... | 398 |
| Receive Total and Transmit Total | 398 |
| Receive and Transmit Size Counters..... | 399 |
| Receive and Transmit Queue Counters | 399 |
| Monitor > Link OAM > Statistics | 401 |
| Receive Total and Transmit Total | 401 |

| | |
|--|-----|
| Monitor > Link OAM > Port Status | 403 |
| Local and Peer | 403 |
| Monitor > Link OAM > Event Status | 405 |
| Monitor > DHCP > Server | 408 |
| Monitor > DHCP > Server > Statistics | 408 |
| Monitor > DHCP > Server > Binding | 410 |
| Monitor > DHCP > Server > Declined IP | 411 |
| Monitor > DHCP > Snooping Table | 412 |
| Monitor > DHCP > Relay Statistics | 414 |
| Monitor > DHCP > Detailed Statistics | 416 |
| Receive and Transmit Packets..... | 417 |
| Monitor > Security > Access Management..... | 419 |
| Monitor > Security > Network > Port Security..... | 420 |
| Port Security > Switch | 420 |
| Port Security > Port | 422 |
| Monitor > Security > Network > NAS | 423 |
| NAS > Switch | 423 |
| NAS > Port..... | 428 |
| Monitor > Security > Network > ACL Status | 434 |
| Monitor > Security > Network > ARP Inspection | 437 |
| Monitor > Security > Network > IP Source Guard | 439 |
| Monitor > Security > AAA | 440 |
| > RADIUS Overview | 440 |
| > RADIUS Details..... | 442 |
| RADIUS Authentication Statistics..... | 442 |
| RADIUS Accounting Statistics..... | 444 |
| Monitor > Security > Switch > RMON | 447 |
| RMON > Statistics | 447 |
| RMON > History | 450 |
| RMON > Alarm | 452 |
| RMON > Event | 454 |
| Monitor > LACP > System Status..... | 455 |
| Monitor > LACP > Port Status | 456 |
| Monitor > LACP > Port Statistics | 457 |
| Monitor > Loop Protection | 458 |
| Monitor > Spanning Tree | 459 |
| Monitor > Spanning Tree > Bridge Status | 459 |
| Bridge Status Details..... | 460 |
| Monitor > Spanning Tree > Port Status | 462 |
| Monitor > Spanning Tree > Port Statistics..... | 464 |
| Monitor > MVR..... | 466 |
| Statistics..... | 466 |
| MVR Channel Groups..... | 467 |
| MVR SFM Information | 468 |
| Monitor > IPMC > IGMP Snooping | 470 |
| IGMP Snooping Status | 470 |
| IGMP Snooping > Groups Information | 473 |
| IGMP Snooping IPv4 SFM Information | 474 |
| Monitor > IPMC > MLD Snooping..... | 476 |
| MLD Snooping > Status | 476 |
| MLD Snooping > Groups Information..... | 478 |
| MLD Snooping > IPv6 SFM Information..... | 479 |
| Monitor > LLDP..... | 481 |
| Monitor > LLDP > Neighbours..... | 481 |
| Monitor > LLDP-MED > Neighbours..... | 483 |
| Monitor > LLDP > Port Statistics | 486 |

| | |
|--|------------|
| Monitor > Ethernet Services | 488 |
| Service Frame (Traffic) Colors - Green / Yellow / Red..... | 488 |
| > EVC Statistics..... | 488 |
| ECE Statistics..... | 490 |
| Monitor > Performance Monitor | 492 |
| Performance Monitor Loss Measurement Statistics..... | 492 |
| Performance Monitor Delay Measurement Statistics | 494 |
| Performance Monitor EVC Statistics..... | 497 |
| Performance Monitor Measurement Interval Information..... | 499 |
| Monitor > PTP..... | 500 |
| External I/O Configuration | 500 |
| External I/O Options | 500 |
| PTP Clock Configuration | 501 |
| Local Clock Current time | 502 |
| Clock Default Dataset..... | 503 |
| Clock current Data Set | 504 |
| Clock Parent Data Set..... | 505 |
| Clock Time Properties Data Set..... | 505 |
| Servo Parameters..... | 506 |
| Filter Parameters | 506 |
| Unicast Slave Configuration | 507 |
| Monitor > MAC Table..... | 510 |
| Monitor > VLANs..... | 512 |
| Monitor > VLANs > VLAN Membership..... | 512 |
| Monitor > VLANs > Ports..... | 514 |
| Monitor > DDMI..... | 517 |
| DDMI > Overview | 517 |
| DDMI > Detailed | 518 |
| Monitor > UDLD | 520 |
| Diagnostics Main Menu | 521 |
| Diagnostics > Ping..... | 521 |
| Ping Procedure..... | 521 |
| Diagnostics > Link OAM > MIB Retrieval | 523 |
| Procedure..... | 523 |
| Diagnostics > Ping6..... | 524 |
| Ping 6 Procedure..... | 524 |
| Diagnostics > VeriPHY | 526 |
| Messages | 527 |
| Diagnostics > Service Activation | 528 |
| Diagnostics > Service Activation > Test..... | 528 |
| Diagnostics > Service Activation > Loopback | 529 |
| Maintenance Menu | 531 |
| Maintenance > Restart Device | 531 |
| Procedure..... | 531 |
| Maintenance > Restart Device > Force Cool Restart..... | 532 |
| Maintenance > Factory Defaults..... | 533 |
| Procedure..... | 533 |
| Maintenance > Software | 534 |
| Software Upload via the Maintenance > Software > Upload Path | 534 |
| Software Upload Procedure | 535 |
| Maintenance > Software > Image Select | 537 |
| Image Select Procedure (Activate Alternate Image)..... | 538 |
| CLI Commands to Re-Access the Web GUI | 539 |
| Maintenance > Software > Peripheral Device Upload | 540 |
| Maintenance > Configuration..... | 541 |
| Industry-standard Configuration Support | 541 |

| | |
|---|------------|
| Save Running Config to Startup-Config | 542 |
| Download Configuration File | 543 |
| Upload a Configuration File | 544 |
| Activate a Configuration File | 546 |
| Delete a Configuration File | 547 |
| 3. Messages and Troubleshooting | 548 |
| S4224 Troubleshooting | 548 |
| EPS Troubleshooting | 548 |
| Protection Types | 549 |
| Failure of Protocol Defects | 549 |
| ERPS Troubleshooting | 550 |
| IPv6 Troubleshooting | 550 |
| Address Resolution in Windows 7 | 550 |
| Verify IPv6 Configuration in Windows 7 | 550 |
| Verify IPv6 Connectivity | 550 |
| IPv6 Auto Config Troubleshooting | 551 |
| RADIUS Troubleshooting in Windows Server Environments | 551 |
| Configure FreeRadius or TACACS+ for Correct ADMIN Level | 552 |
| AAA 'keyword attribute' | 552 |
| Troubleshooting High CPU Load Conditions | 553 |
| Normal Conditions Causing High CPU Load | 554 |
| For Additional High CPU Load TS Information | 554 |
| S4224 Error Recovery | 555 |
| Web Interface Messages | 557 |
| System Log Messages | 594 |
| <i>Informational</i> Level Messages | 594 |
| <i>Warning</i> Level Messages | 594 |
| <i>Error</i> Level Messages | 595 |
| <i>Notice</i> Level Messages | 595 |
| Third Party Program Messages | 596 |
| Appendix A - Cables and Connectors | 599 |
| Appendix B - Licenses | 601 |
| Appendix C: Application Notes | 613 |
| S4224 Applications Support | 613 |
| Available TN S4224 Application Notes | 613 |
| Appendix D: Service, Warranty & Compliance Information | 614 |
| Appendix E: SNMP Traps and MIBs | 615 |
| MIBs Supported | 615 |
| tn-mibs-v2.2.0.zip file | 616 |
| For Additional MIB Information | 622 |
| Glossary | 630 |
| Index | 666 |

Figures

| | |
|---|-----|
| Figure 1. SNMP v3 Users, Groups, and Views..... | 69 |
| Figure 2. Spanning Tree Example | 157 |
| Figure 3. Multiple Spanning Tree Example..... | 157 |
| Figure 4. 802.1Q EtherTypes (excerpt from IEEE 802.1ad 2005)..... | 272 |
| Figure 5. All to one bundling VLAN Cases..... | 272 |
| Figure 6. S-VLAN with multiple trunks (EPL service at 3 different UNIs) | 273 |
| Figure 7. S-VLAN with one trunk (Multiple UNI bundled at the Operator domain) | 273 |
| Figure 8. Provider Bridge E-LINE Service | 291 |
| Figure 9. Provider Bridge E-LINE Service | 291 |
| Figure 10. Color Aware Token Bucket Profile for Bandwidth Profiling | 312 |
| Figure 11. Example SLA for Bandwidth profiling | 313 |
| Figure 12. Connector Types..... | 600 |

Tables

| | |
|---|-----|
| Table 1. EAPOL Counters..... | 430 |
| Table 2. Backend Server Counters..... | 431 |
| Table 3. Last Supplicant/Client Information | 432 |
| Table 4: Syslog <i>Informational</i> Messages | 594 |
| Table 5: Syslog <i>Warning</i> Messages | 594 |
| Table 6: Syslog <i>Error</i> Messages | 595 |
| Table 7: Syslog <i>Notice</i> Messages..... | 595 |
| Table 8: Connector Descriptions..... | 600 |
| Table 9: Public MIBs | 617 |
| Table 10: Private MIBs..... | 620 |
| Table 11: Traps List | 623 |

1. Introduction

Transition Networks' Carrier Ethernet solution delivers the promise of simplicity deployed. This comprehensive solution includes CE 2.0 compliant demarcation devices, access switches, and the Converge™ element and service management platform.

The **S4140** is a 10GE Carrier Ethernet NID. The S4140 provides four 1Gbps/10GE SFP+ ports and it includes IEEE 1588v2, SyncE, and Service Activation Test generation. The S4140 CE NID has four 1G/10G SFP+ interfaces with DMI support (1000X, SGMII, 10G), Sync-E IN/OUT, and IEEE 1588 IN/OUT ports.

The **S4212** access switch has twelve 100/1000Mbps ports and two 10GE uplinks. The S4212 access switch includes IEEE 1588v2, SyncE, and Service Activation Test generation.

The **S4224** access switch has twenty-four 100/1000Mbps ports and four 10GE uplinks. The S4224 includes IEEE 1588v2, SyncE, and Service Activation Test generation.

The S4140/S4212/S4224 (hereafter "**S4xxx**") software provides a rich set of Carrier Ethernet services, Ethernet switching, and Ethernet transport features. Advanced TCAM-based QoS processing enables delivery of differentiated services with per-service SLA guarantees. Security is assured via separate processing using the S4xxx internal processor. The TN S4xxx is designed to support a wide range of MEF-based Carrier Ethernet services for Mobile Backhaul, Business Ethernet, Cloud Assurance and Carrier Exchange E-Access Services.

Transition Networks' Carrier Ethernet portfolio meets the demand for highly scalable, on-demand, dynamic bandwidth, differentiated services (E-Line E-LAN, E-Access), and integration of Cloud services in a fully automated service centric management platform , Converge™ , to ensure robust performance SLA reporting and end-to-end pro-active fault management.

See the applicable Install Guide manual for S4xxx features, models, specifications, and installation.

Document Overview

The purpose of this manual is to provide information on the configuration, monitoring, diagnostics, and maintenances of the TN S4140, S4224, and S4212 .

The procedures in this manual require you to have completed the install procedure in the S4140 Install Guide manual. This manual documents all of the S4xxx models, and notes differences where they apply. This manual includes four chapters, five appendixes, a table of contents, a glossary, and an index.

A printed documentation postcard is shipped with each S4xxx device. Context-sensitive Help screens are built into the Web interface. A substantial set of technical documents, white papers, case studies, application notes, etc. are available on the Transition Networks web site at www.transition.com. Note that this manual may provide links to third party web sites for which Transition Networks, Inc. is not responsible.

Related Manuals and Online Help

This manual is one of several S4224 manuals which include:

- S4224 Install Guide, 33557 (this manual)
- S4224 Quick Start Guide, 33636 (printed)
- S4224 User Guide, 33558
- S4224 CLI Reference, 33559
- RFC2544 User Guide, 33638
- Converge™ EMS Windows Install Guide (33543), Linux Install Guide (33533), Admin Procedures (33544)
- Release Notes (version specific)

For Product Information, Application Notes, etc., check the S4224 landing page at <http://www.transition.com/TransitionNetworks/Landing/S4224/S4224.aspx>

For access to the latest S4224 datasheet, Features, Applications, Specs, SKUS, etc., check the S4224 product page at <http://www.transition.com/TransitionNetworks/Products2/Family.aspx?Name=S4224>.

Context-sensitive Help screens are built into the Web interface (click ) and the CLI (type ? or **Help**).

Check the TN web site at <http://www.transition.com/> for additional white papers, application notes, etc.

2. Web Interface Menu System

The S4xxx Web interface menu system is shown below in terms of its sub-menus and functions.

| Main Menu | Configuration sub-menu | Monitor sub-menu | Diagnostics sub-menu | Maintenance sub-menu |
|--|--|---|---|---|
| <ul style="list-style-type: none"> ▶ Configuration ▶ Monitor ▶ Diagnostics ▶ Maintenance | <ul style="list-style-type: none"> ▼ Configuration <ul style="list-style-type: none"> ▶ System ▶ Ports ▶ DHCP ▶ Security ▶ Aggregation ▶ Link OAM ▪ Loop Protection ▶ Spanning Tree ▶ IPMC Profile <ul style="list-style-type: none"> ▪ MVR ▶ IPMC <ul style="list-style-type: none"> ▪ L2CP ▶ LLDP ▪ EPS ▪ MEP ▪ ERPS ▪ MAC Table ▶ VLAN Translation <ul style="list-style-type: none"> ▪ VLANs ▶ Private VLANs ▶ VCL ▶ Ethernet Services ▶ Performance Monitor ▶ QoS <ul style="list-style-type: none"> ▪ Mirroring ▪ PTP ▶ GVRP ▶ Service Activation ▶ DDMI ▪ UDLD | <ul style="list-style-type: none"> ▼ Monitor <ul style="list-style-type: none"> ▶ System ▶ Ports ▶ Link OAM ▶ DHCP ▶ Security ▶ LACP <ul style="list-style-type: none"> ▪ Loop Protection ▶ Spanning Tree ▶ MVR ▶ IPMC ▶ LLDP ▶ Ethernet Services ▶ Performance Monitor <ul style="list-style-type: none"> ▪ PTP ▪ MAC Table ▶ VLANs ▶ DDMI ▪ UDLD | <ul style="list-style-type: none"> ▼ Diagnostics <ul style="list-style-type: none"> ▪ Ping ▶ Link OAM ▪ Ping6 ▪ VeriPHY ▶ Service Activation | <ul style="list-style-type: none"> ▼ Maintenance <ul style="list-style-type: none"> ▪ Restart Device ▪ Factory Defaults ▼ Software <ul style="list-style-type: none"> ▪ Upload ▪ Image Select ▪ Peripheral Device Upload ▼ Configuration <ul style="list-style-type: none"> ▪ Save startup-config ▪ Download ▪ Upload ▪ Activate ▪ Delete |

The four Main menu selections are:

- **Configuration** - lets you define system operating parameters for the available S4224 features.
- **Monitor** - lets you view and track the S4xxx operating functions. See ‘[Monitor](#)’ on page 380.
- **Diagnostics** - provides access to the full set of S4xxx tests and verification functions. See “[Diagnostics Main Menu](#)’ on page 521.
- **Maintenance** - supports S4xxx troubleshooting and service functions. See “[Maintenance Menu](#)” on page 531.

Click one or more of the main menu selections to display its sub-menus. Note that some sub-menus vary between the S4xxx models.

Each of these sub-menus and their functions are described in the following sections. Note that certain features may have separate manuals each with its own Web GUI and CLI descriptions and procedures.

Menu Bar Icons

These icons display in the top right corner of each S4224 web GUI screen.

Home **Logout** **Show Help**



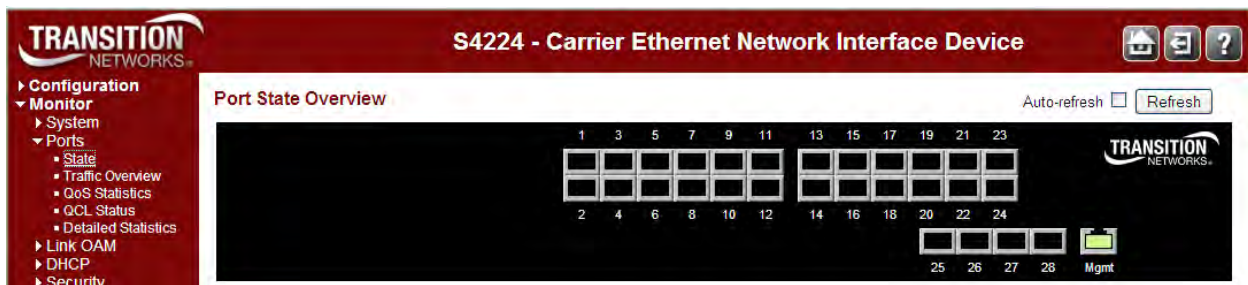
Home: Displays the S4xxx Startup Screen from the **Monitor > Ports > State** menu path.

Logout: Display the confirmation message “*Do you want to log out of the web site?*”. Click the **OK** button to clear the web page message, perform a logout, and re-display the login (Username/Password) screen.

Show Help: Displays the related online Help screen in a new window,

Startup Screen

At system startup and after a re-boot, the Port State Overview page displays from the **Monitor > Ports > State** menu path.



The four Main menu selections are shown and described in the following sections.

Configuration Main Menu

Configuration > System

The S4xxx system information is configured from the **Configuration > System** menu path. Here you can configure S4xxx device level Information, IP, NTP, time, and logging.

System Information Configuration

| | |
|-----------------|--|
| System Contact | <input style="width: 80%;" type="text"/> |
| System Name | <input style="width: 80%;" type="text"/> |
| System Location | <input style="width: 80%;" type="text"/> |

The S4xxx system information parameters are explained below.

System Contact

Enter the textual identification of the contact person for this managed node, together with information on how to contact this person. The valid string length is 0 to 255 characters, and the allowed content is the set of ASCII characters from 32 to 126. In the ASCII code table, the characters from 32 to 126 inclusive are printable. (The ASCII characters from 0 to 32 and 127 are defined as control characters and are not printable.) This field is blank by default.

If you delete an existing System Contact entry, the message “*System Contact is empty. Do you want to proceed anyway?*” displays. Verify the action and continue operation.

System Name

Enter an administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z, a-z), digits (0-9), minus sign (-).

No space characters are permitted as part of a name. The first character must be an alpha character, and the first or last character must not be a minus sign. The valid string length is 0 to 255 characters. This field is blank by default.

If you delete an existing System Name entry, the message “*System Name is empty. Do you want to proceed anyway?*” displays. Verify the action and continue operation. Note that you can not access the S4224 by System Name via DHCP/DNS.

System Location

The physical location of this node (e.g., *telephone closet, 3rd floor*). The valid string length is 0 to 255 characters, and the allowed content is the set of ASCII characters from 32 to 126. In the ASCII code table, the characters from 32 to 126 inclusive are printable. (The ASCII characters from 0 to 32 and 127 are defined as control characters and are not printable.) This field is blank by default.

If you delete an existing System Location entry, the message “*System Location is empty. Do you want to proceed anyway?*” displays. Verify the action and continue operation.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

An updated System Information Configuration table is shown below.

| System Information Configuration | |
|----------------------------------|---------------------|
| System Contact | JEdgar |
| System Name | SCENID010 |
| System Location | 10690RedCircleDrive |

Save Reset

Note that changes in the Web interface here will change the CLI prompt appearance. Based on the screen above, the CLI prompt will change to include the newly added System Name:

```
from: >
to: SCENID010: />
```

If you enter a space character or other invalid entry and click the **Save** button, the message "'System Name' is not valid. Please refer to the help page for the valid format." displays.

| System Information Configuration | |
|----------------------------------|--------------------|
| System Contact | JEdgar |
| System Name | SCEN ID 010 |
| System Location | 10690 Red Circle D |

Save Reset

Message from webpage

! 'System Name' is not valid. Please refer to the help page for the valid format.

OK

Click the **OK** button to clear the webpage message, enter the System Name without any spaces, and click the **Save** button.

Character Support Note

The S4224 supports the Space * < > : % / \ " ? |, and all other keyboard characters. The S4224 supports an individual "dot" character, but does not support consecutive dots (e.g., it supports A.B.C.bin, but does not support ABC....bin).

IP Configuration

Configure IP basic settings, control IP interfaces and IP routes from the **Configuration > System > IP** menu path. The maximum number of interfaces supported is 128 and the maximum number of routes is 32. The default System IP Configuration page is shown below.

IP Configuration

| | |
|--------------|--------------------------|
| Mode | Host |
| DNS Server 0 | No DNS server |
| DNS Server 1 | No DNS server |
| DNS Server 2 | No DNS server |
| DNS Server 3 | No DNS server |
| DNS Proxy | <input type="checkbox"/> |

IP Interfaces

| Delete | VLAN | DHCPv4 | | | IPv4 | | DHCPv6 | | | IPv6 | |
|--------------------------|------|--------------------------|----------|---------------|--------------|-------------|--------------------------|--------------------------|---------------|---------|-------------|
| | | Enable | Fallback | Current Lease | Address | Mask Length | Enable | Rapid Commit | Current Lease | Address | Mask Length |
| <input type="checkbox"/> | 1 | <input type="checkbox"/> | 0 | | 192.168.1.11 | 24 | <input type="checkbox"/> | <input type="checkbox"/> | | | |

Add Interface

IP Routes

| Delete | Network | Mask Length | Gateway | Next Hop VLAN |
|-----------|---------|-------------|---------|---------------|
| Add Route | | | | |

Save Reset

The parameters are described below.

IP Configuration

Mode

Configure whether the IP stack should act as a **Host** or a **Router**. In **Host** mode, IP traffic between interfaces will not be routed. In **Router** mode traffic is routed between all interfaces.

DNS Server

This setting controls the DNS name resolution done by the switch. There are four servers available for configuration, and the index of the server presents the preference (less index has higher priority) in doing DNS name resolution. The system selects the active DNS server from configuration in turn, if the preferred server does not respond in five attempts. The following modes are supported:

No DNS server : No DNS server will be used.

Configured IPv4 : Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation. Make sure the configured DNS server could be reachable (e.g. via PING) for activating DNS service.

Configured IPv6 : Explicitly provide the valid IPv6 unicast (except linklocal) address of the DNS Server. Make sure the configured DNS server could be reachable (e.g. via PING6) for activating DNS service.

From any DHCPv4 interfaces : The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface is used.

From this DHCPv4 interface : Specify from which DHCPv4-enabled interface a provided DNS server should be preferred.

From any DHCPv6 interfaces : The first DNS server offered from a DHCPv6 lease to a DHCPv6 enabled interface will be used.

From this DHCPv6 interface : Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.

| |
|----------------------------|
| No DNS server |
| Configured IPv4 or IPv6 |
| From any DHCPv4 interfaces |
| From this DHCPv4 interface |
| From any DHCPv6 interfaces |
| From this DHCPv6 interface |

DNS Proxy

When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network. Only IPv4 DNS proxy is now supported.

IP Interfaces

Delete

Select this option to delete an existing IP interface.

VLAN

The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.

DHCPv4 Enable

Enable the DHCPv4 client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol. The DHCPv4 client will announce the configured System Name as hostname to provide DNS lookup.

DHCPv4 Fallback Timeout

The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.

DHCPv4 Current Lease

For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.

IPv4 Address

The IPv4 address of the interface in dotted decimal notation. If **DHCP** is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

IPv4 Mask Length

The IPv4 network mask, in number of bits (*prefix length*). Valid values are 0 - 30 bits for an IPv4 address.

If **DHCP** is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

DHCPv6 Enable

Enable the DHCPv6 client by checking this box. If this option is enabled, the system will configure the IPv6 address of the interface using the DHCPv6 protocol.

DHCPv6 Rapid Commit

Enable the DHCPv6 Rapid-Commit option by checking this box. If this option is enabled, the DHCPv6 client terminates the waiting process as soon as a Reply message with a Rapid Commit option is received. This option is only manageable when a DHCPv6 client is enabled.

DHCPv6 Current Lease

For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.

IPv6 Address

The IPv6 address of the interface. A IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, **fe80::215:c5ff:fe03:4dc7**. The symbol **::** is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address.
The field may be left blank if IPv6 operation on the interface is not desired.

IPv6 Mask

The IPv6 network mask, in number of bits (*prefix length*). Valid values are between 1 and 128 bits for a IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.

Resolving IPv6 DAD

The link-local address is formed from an interface identifier based on the hardware address which is supposed to be uniquely assigned. Once the DAD (Duplicate Address Detection) detects the address duplication, the operation on the interface SHOULD be disabled.
At this moment, manual intervention is required to resolve the address duplication. For example, check whether the loop occurs in the VLAN or there is indeed other device occupying the same hardware address as the device in the VLAN.
After making sure the specific link-local address is unique on the IPv6 link in use, delete and then add the specific IPv6 interface to restart the IPv6 operations on this interface.

IP Routes

Delete

Select this option to delete an existing IP route.

Network

The destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value **0.0.0.0** or IPv6 **::** notation.

Mask Length

The destination IP network or host mask, in number of bits (*prefix length*). It defines how much of a network address that must match, in order to qualify for this route. Valid values are **0** - **32** bits for IPv4 routes or **0** - **128** for IPv6 routes. Only a default route will have a mask length of **0** (match anything).

Gateway

The IP address of the IP gateway. Valid format is dotted decimal notation or a valid IPv6 notation. The Gateway and Network must be of the same type.

IP Routes

| Delete | Network | Mask Length | Gateway | Next Hop VLAN |
|--------|---------|-------------|----------|---------------|
| Delete | 0.0.0.0 | 0 | 10.0.1.1 | 0 |

It may be necessary to add a static route if a default gateway is required or if the device does not reside within the same network. Routing can then be enabled at **System > IP > IP Configuration**. See the *Static IP Routing (SIR) User Guide*, 33542 for the Static Routing function descriptions and procedures. A default route (AKA, gateway of last resort) is the network route used by a router when no other known route exists for an IP packet's destination address (Network = 0.0.0.0, Mask Length = 0, Gateway 10.0.1.1 as shown above).

Next Hop VLAN

The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.

If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway.

If the IPv6 gateway address is not link-local, the system ignores the next hop VLAN for the gateway.

When DNS Proxy is enabled, the S4xxx will relay DNS requests to the currently configured DNS server on the S4xxx, and reply as a DNS resolver to the client device on the network.

Note that setting these fields does not provide the full set of IP, BootP, VLAN, DNS server, and Management VLAN / member ports configuration. See the related Configuration sections of this manual for additional information.

Buttons

Add Interface: Click to add a new IP interface. A maximum of 8 interfaces is supported.

Add Route: Click to add a new IP route. A maximum of 32 routes is supported.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Messages

After you click the **Renew** button, the message “*Warning: When renewing DHCP you may lose IP connectivity. Do you want to continue?*” displays.

If you are sure you want to do this, click the **OK** button to clear the webpage message.

If you do not want to renew DHCP / lose the IP connection, click the **Cancel** button and continue operation.

After you click the **Save** button, the message “*Warning: When changing parameters on this page, you may lose IP connectivity. This could in turn require reconfiguration of this PC. Do you want to continue?*” displays.

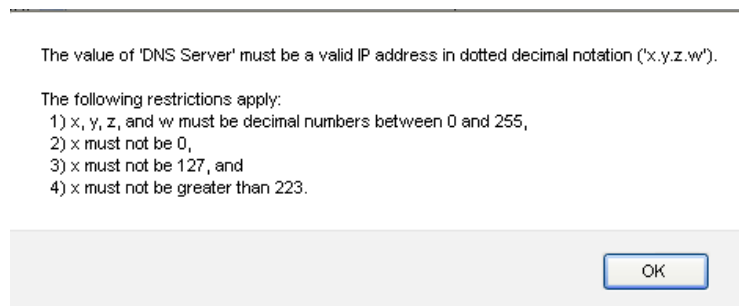
If you are sure you want to change these parameters, click the **OK** button to clear the webpage message, and then follow any on-screen messages.

If you do not want to change parameters, click the **Cancel** button and continue operation.

Message: The value of ‘DNS Server’ must be a valid IP address in dotted decimal notation (‘x.y.z.w’).

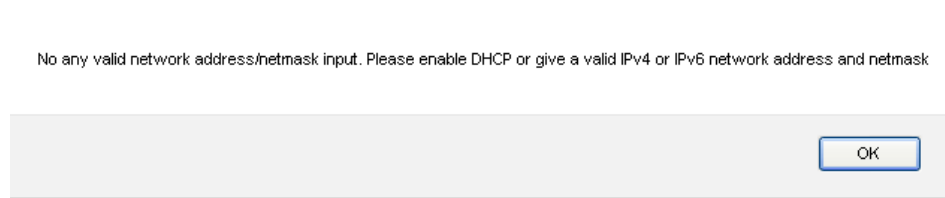
The following restrictions apply:

- 1) x, y, z, and w must be decimal numbers between 0 and 255,
- 2) x must not be 0,
- 3) x must not be 127, and
- 4) x must not be greater than 223.



Recovery: 1. Click the **OK** button to clear the message. 2. Re-enter a valid IP address per the on-screen instructions.

Message: No any network address/netmask input. Please enable DHCP or give a valid IPv4 or IPv6 network address and netmask.



Recovery: 1. Click the **OK** button to clear the message. 2. Re-enter a parameter per the instructions.

Message: A static address is only used if the fall-back time-out is non-zero.



Recovery: 1. Click the **OK** button to clear the message. 2. Re-enter the Fallback parameter with a value greater than 1.

NTP Configuration

Configure NTP on this page from **Configuration > System > NTP**. Network Time Protocol (NTP) is a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

The S4xxx uses NTP for real time clock synchronization with the network time server. The NTP is compliant with RFC 5905. The S4xxx takes care of daylight saving options where used.

The S4xxx management interfaces provide options to configure NTP and report the network time synchronized. The RFC 5905time obtained is used for all RFC 5905services that need a timestamp. Note that you can not access the S4xxx by System Name via DHCP/DNS.

| Mode | Disabled |
|----------|----------|
| Server 1 | |
| Server 2 | |
| Server 3 | |
| Server 4 | |
| Server 5 | |

Save Reset

Mode

Sets / indicates NTP mode operation, either:

Enabled: Enable NTP mode operation. When NTP mode operation is enabled, the agent forwards NTP messages between the clients and the server when they are not on the same subnet domain.

Disabled: Disable NTP mode operation.

Server

Provide the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'. In addition, it can also accept a domain name address. Note that you can 'cut and paste' information to and from this field.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Messages

Parameter <server_ipv6> doesn't allowed all zero or all 'ff'

Sever already exist! Delete it first.

Using IPv6 multicast address is not allowed here.

Time Configuration

This page allows you to configure the Time Zone and Daylight Savings Time (DST) parameters from the **Configuration > System > Time** menu path.

Time Zone Configuration

| | |
|--------------------------------|-----------------------|
| Time Zone Configuration | |
| Time Zone | None |
| Acronym | (0 - 16 characters) |

Daylight Saving Time Configuration

| | |
|----------------------------------|----------|
| Daylight Saving Time Mode | |
| Daylight Saving Time | Disabled |

Start Time settings

| | |
|---------|------|
| Month | Jan |
| Date | 1 |
| Year | 2000 |
| Hours | 0 |
| Minutes | 0 |

End Time settings

| | |
|---------|------|
| Month | Jan |
| Date | 1 |
| Year | 2000 |
| Hours | 0 |
| Minutes | 0 |

Offset settings

| | |
|--------|----------------------|
| Offset | 1 (1 - 1440) Minutes |
|--------|----------------------|

Save Reset

The Time Zone and Daylight Savings Time (DST) parameters are described below.

Time Zone Configuration

Time Zone

Time Zone: Lists various Time Zones world wide. Select the appropriate Time Zone from the drop down and click Save to set. See the end of this section for the Time Zone selections.

Acronym: User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. Enter up to 16 alpha-numeric characters including '-', ' ' or '.' characters.

Daylight Saving Time Configuration

Daylight Saving Time

This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. The default is **Disabled**.

Select **Disabled** to disable the Daylight Saving Time configuration.

Select **Recurring** and configure the Daylight Saving Time duration to repeat the configuration every year.

Select **Non-Recurring** and configure the Daylight Saving Time duration for single time configuration.

Recurring Configurations

Start Time Settings

Week - Select the starting week number (1-5).

Day - Select the starting day (Sun, Mon, Tue, Wed, Thu, Fri, Or Sat).

Month - Select the starting month (Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Or Dec).

Hours - Select the starting hour (0 - 23).

Minutes - Select the starting minute (0 - 59).

End Time Settings

Week - Select the ending week number (1-5).

Day - Select the ending day (Sun, Mon, Tue, Wed, Thu, Fri, Or Sat).

Month - Select the ending month (Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Or Dec).

Hours - Select the ending hour (0 - 23).

Minutes - Select the ending minute (0 - 59).

Offset Settings

Offset - Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

Start Time Settings

Month - Select the starting month (Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Or Dec).

Date - Select the starting date (1 - 31).

Year - Select the starting year (2000 - 2097).

Hours - Select the starting hour (0 - 23).

Minutes - Select the starting minute (0 - 59).

End Time Settings

Month - Select the ending month (Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Or Dec).

Date - Select the ending date (1 - 31).

Year - Select the ending year (2000 - 2097).

Hours - Select the ending hour (0 - 23).

Minutes - Select the ending minute (0 - 59).

Offset Settings

Offset - Enter the number of minutes to add during Daylight Saving Time (1 - 1440).

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Time Zones List

The various Time Zone selections available world wide are listed below.

None

(GMT-12:00) International Date Line West

(GMT-11:00) Midway Island, Samoa

(GMT-10:00) Hawaii

(GMT-09:00) Alaska

(GMT-08:00) Pacific Time (US and Canada)

(GMT-08:00) Tijuana, Baja California

(GMT-07:00) Arizona

(GMT-07:00) Chihuahua, La Paz, Mazatlan - New

(GMT-07:00) Chihuahua, La Paz, Mazatlan - Old

(GMT-07:00) Mountain Time (US and Canada)

(GMT-06:00) Central America

(GMT-06:00) Central Time (US and Canada)

(GMT-06:00) Guadalajara, Mexico City, Monterrey - New

(GMT-06:00) Guadalajara, Mexico City, Monterrey - Old

(GMT-06:00) Saskatchewan

(GMT-05:00) Bogota, Lima, Quito, Rio Branco

(GMT-05:00) Eastern Time (US and Canada)

(GMT-05:00) Indiana (East)

(GMT-04:30) Caracas

(GMT-04:00) Atlantic Time (Canada)

(GMT-04:00) La Paz

(GMT-04:00) Manaus

(GMT-04:00) Santiago

(GMT-03:30) Newfoundland

(GMT-03:00) Brasilia

(GMT-03:00) Buenos Aires

(GMT-03:00) Georgetown

(GMT-03:00) Greenland

(GMT-03:00) Montevideo

(GMT-02:00) Mid-Atlantic

(GMT-01:00) Azores

(GMT-01:00) Cape Verde Is.

(GMT) Casablanca

(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

(GMT) Monrovia, Reykjavik

(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

(GMT+01:00) Brussels, Copenhagen, Madrid, Paris

(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb

(GMT+01:00) West Central Africa

Log (System Log) Configuration

Configure System Logging (Syslog) on this page from **Configuration > System > Log**. The Syslog data is stored in RFC 5905RAM by default. Syslog data will be lost with an RFC 5905reboot unless other provisions are made to save it.

For syslog monitoring details, see 'Monitor > System > Log' on page 387.

Server Mode

Sets / indicates the server mode operation. When Server Mode is enabled, the syslog message will be sent out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always be sent out, even if the syslog server does not exist. Possible modes are:

Enabled: Enable server mode operation.

Disabled: Disable server mode operation.

Server Address

Sets / indicates the IPv4 or IPv6 host address of the syslog server. If the switch provides the DNS feature, it can also be a host name. If you enter an invalid address, or do not enter any address, the message "The format of Server Address is invalid" displays. Re-enter a valid IPv4 or IPv6 server address.

Syslog Level

Sets / indicates what kind of message will be sent to the syslog server. Possible modes are:

Error: Send the specific messages which severity code is less or equal than Error(3).

Warning: Send the specific messages which severity code is less or equal than Warning(4).

Notice: Send the specific messages which severity code is less or equal than Notice(5).

Informational: Send the specific messages which severity code is less or equal than Informational(6).

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Syslog Events

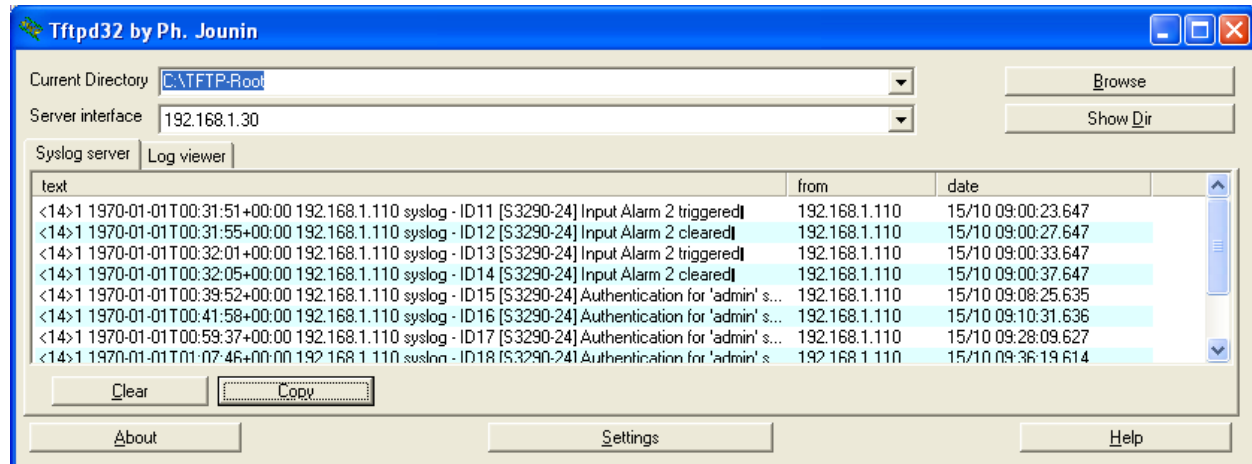
Syslog events supported include:

- Port 1 link up and down
- Port Security Limit Control reach but the action is none
- IP source guard table is full
- IP source guard table reaches the port limitation.
- IP source guard port limitation changes, should delete entry
- S4224 boot up
- SNMP authentication failure

Examples

```
<14>1 1970-01-01T04:57:31+00:00 192.168.1.110 syslog - ID6564 [S4224-24] Input Alarm '1'
triggered and message is 'AlArM1' 192.168.1.110 30/09 12:57:46.977

<14>1 1970-01-01T00:31:51+00:00 192.168.1.110 syslog - ID11 [S4224-24] Input Alarm 2 triggered
192.168.1.110 15/10 09:00:23.647
<14>1 1970-01-01T00:31:55+00:00 192.168.1.110 syslog - ID12 [S4224-24] Input Alarm 2 cleared
192.168.1.110 15/10 09:00:27.647
<14>1 1970-01-01T00:32:01+00:00 192.168.1.110 syslog - ID13 [S4224-24] Input Alarm 2 triggered
192.168.1.110 15/10 09:00:33.647
<14>1 1970-01-01T00:32:05+00:00 192.168.1.110 syslog - ID14 [S4224-24] Input Alarm 2 cleared
192.168.1.110 15/10 09:00:37.647
<14>1 1970-01-01T00:39:52+00:00 192.168.1.110 syslog - ID15 [S4224-24] Authentication for
'admin' successful via 'http'192.168.1.110 15/10 09:08:25.635
```



Ports Configuration

This page displays current port configurations and allows S4224 shared port and port configuration and DMI configuration from the **Configuration > Ports** menu path.

All Ethernet ports are equipped with LEDs for visual status of speed, duplex and activity. The 10/100/1000BaseT ports provide standard features such as configuring Auto negotiation, Advertisement capabilities, speed, duplex, flow control and autocross. These features are compliant with the IEEE 802.3-2008 Ethernet PHYs standards.

The SFP port when in 100BaseFx mode is set at 100Mbps and the duplex mode can be user configured. Far End Fault (FEF) is supported in this mode of operation. The SFP port when in 1000BaseX mode always has Auto-negotiation and Auto-negotiation Bypass modes enabled. Flow control is configurable. The SFP port can operate in SGMII mode with Auto-negotiation always on. When the SFP ports operate in 100BaseFx mode, the optical link integrity can be identified by FEF. This is very useful to detect faults in network since fiber links can be long. FEF is enabled by default and is not a configurable option.

Configuration > Ports > Shared Port Configuration

Configure the FPGA Shared Port on this page.



The parameters are:

Shared Port (24) Mode

This switch contains one port that is 'Shared'. On the S4224 products, port 24 is shared. The Shared Port has two modes.

In **External** mode, the port can work as normal port.

In **Internal** mode is, the port is just used for RFC 2544 testing, and it can not be user configured.

Shared Port Status

Sets the Shared Port operating mode. Possible modes are:

Internal: This mode disconnects the the Shared Port from the SFP interface and attaches it internally to to an FPGA. No connectivity can be achieved through the Shared Port's SFP interface while in this mode.

External: This is the default mode. In this mode, the shared port is attached to the SFP interface, and works like the rest of the ports on this switch.

The Shared Port mode must be set to **External** for normal port function and **Internal** for the following features to work:

Diagnostics > Service Activation > Test
Diagnostics > Service Activation > Loopback

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Configuration > Ports > Configuration

The RFC 5905 ports can be configured here in terms of speed, flow control, max. frame size, excessive collision control, and port description.

| Port | Link | Speed | | Adv Duplex | | Adv speed | | | Flow Control | | | Maximum Frame Size | Excessive Collision Mode | Description |
|------|------|---------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|---------|---------|--------------------|--------------------------|-------------|
| | | Current | Configured | Fdx | Hdx | 10M | 100M | 1G | Enable | Curr Rx | Curr Tx | | | |
| * | | | <> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | 10056 | <> | |
| 1 | Down | Auto | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | ? | | 10056 | | |
| 2 | Down | Auto | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | ? | | 10056 | | |
| 3 | Down | Auto | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | ? | | 10056 | | |
| 4 | Down | Auto | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | ? | | 10056 | | |
| 5 | Down | Auto | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | ? | | 10056 | | |
| 6 | Down | Auto | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | ? | | 10056 | | |
| 7 | Down | Auto | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | ? | | 10056 | | |
| 8 | Down | Auto | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | ? | | 10056 | | |
| 9 | Down | Auto | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | ? | | 10056 | | |
| 10 | Down | Auto | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | ? | | 10056 | | |
| 11 | Down | Auto | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | ? | | 10056 | | |
| 12 | Down | Auto | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | ? | | 10056 | | |
| 13 | Down | Auto | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | ? | | 10056 | | |
| 14 | Down | Auto | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | ? | | 10056 | | |
| 15 | Down | Auto | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | | ? | | 10056 | | |

The Port Configuration parameters are explained below.

Port

This is the logical port number for this row. The * in the Port column acts as a 'wild card' character which causes the selections in this row to be applied to all other Ports (rows) in the table for which this selection is valid.

Link

The current link state is displayed graphically. Green indicates the link is up and red that it is down.

Current Link Speed

Provides the current link speed of the port:

100fdx: the link is up and operating at 100 Mbps at Full Duplex.

Down: the link is currently down.

[s] : Shared port (lower case "s").

[S] : Active shared port (upper case "S").

Configured Link Speed

Select any available link speed for the given S4224 port. The available selections are **Disabled**, **Auto**, **10Mbps HDX**, **10Mbps FDX**, **100Mbps HDX**, **100Mbps FDX**, **1Gbps FDX** and **10Gbps FDX**.

Depending on the type of port, (copper or SFP), this can be displayed as:

<>: Displays in the 'wild card' row to indicate no parameter selection has been made yet.

Auto: Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.

Disabled: administratively disables the S4224 port operation.

10Mbps HDX - Forces the port in 10Mbps half duplex mode.

10Mbps FDX - Forces the port in 10Mbps full duplex mode.

100Mbps HDX - Forces the port in 100Mbps half duplex mode.

100Mbps FDX - Forces the port in 100Mbps full duplex mode.

1Gbps FDX - Forces the port in 1Gbps full duplex

10Gbps FDX - Forces the port in 10Gbps full duplex mode.

The 10/100/1000BaseT and 100BaseFx/1000BaseX/SGMII ports support auto-negotiation per the IEEE 802.3 standard. The ports come up in Auto-negotiation mode by default.

The 10/100/1000BaseT also supports disabling Auto-negotiation and can be forced to 10 half, 10 full, 100 half, 100 full or 1G full-duplex modes. When auto negotiation parallel detects a forced mode remote, it defaults to the link speed and Half duplex. This can result in a forced Full duplex port talking to an Auto port operating in Half duplex mode, resulting in excessive collision issues.

The Auto-negotiation signaling is compliant with IEEE802.3 2008 Clause 28. In 1000BaseX mode, auto negotiation is always enabled, in a case where the link partner doesn't auto negotiate, the bypass mode is activated automatically to link at 1000Mbps and full duplex (1Gbps FDX).

The Auto-negotiation signaling is compliant with IEEE802.3 2008 Clause 37. In 100BaseFx mode, auto-negotiation is not supported and the ports come up in forced 100M/Full-duplex. Duplex is configurable to half or full to support legacy equipment.

Advertise Duplex (HDX / FDX)

When duplex is set as auto (Autonegotiation), the port will only advertise the specified duplex as either Fdx or Hdx to the link partner. By default, the port will advertise all the supported duplexes if the Duplex is set to 'Auto'.

Advertise Speed

When Speed is set as auto (Autonegotiation), the port will only advertise the specified speeds (Speed10 Speed100 Speed1000) to the link partner. By default port will advertise all the supported speeds if speed is set as Auto.

Flow Control

When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner.

When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto Negotiation.

Check the **Enable** checkbox to use flow control. This setting is related to the setting for Configured Link Speed.

Note: The 100FX standard doesn't support Auto Negotiation, so when in 100FX mode the flow control capabilities will always be shown as "disabled".

Maximum Frame Size

Enter the maximum frame size to be allowed for the S4224 port, including FCS. The valid range is 1518-10056 bytes. The default is 10056 bytes for all ports.

Excessive Collision Mode

Configure port transmit collision behavior:

<>: wild card character selects all.

Discard: Discard frame after 16 collisions (default).

Restart: Restart the backoff algorithm after 16 collisions.

The Excessive Collision Mode parameter does not apply to the fiber ports.

Description

Lets you enter a definitive description for each port. This is the Port description string to uniquely identify the circuit, using a maximum of 255 alphanumeric characters.

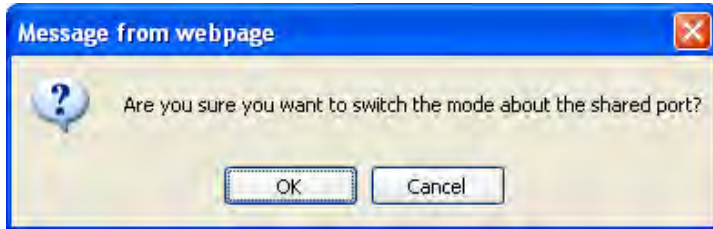
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page. Any changes made locally will be undone.

Messages: Are you sure you want to switch the mode about the shared port?



DHCP Configuration

Configuration > DHCP

The **Configuration > DHCP** menu path lets you configure S4224 DHCP Server, DHCP Snooping, and DHCP Relay parameters.

DHCP (Dynamic Host Configuration Protocol) is used for assigning dynamic IP addresses to devices on a network. DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). The IP address pool management is done by the server and not by a person.

The **Configuration > DHCP** menu path lets you configure S4224 DHCP Snooping and/or DHCP Relay, as discussed below. Note that you can not access the S4224 by System Name via DHCP/DNS.

Note: for DHCP server operation, you must also configure parameters at **Configuration > System > IP**. See [IP Configuration](#) on page 18.

Configuration > DHCP > DHCP Server

This menu path lets you configure the DHCP Server's **Mode**, **Excluded IP**, and **Pool** functions.

> DHCP Server Mode

This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN. A DHCP Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP client.

Click the **Add VLAN Range** button to display the entry fields.

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

Configuration > DHCP > Server

DHCP Server Mode Configuration

Global Mode

Mode: Disabled

VLAN Mode

| Delete | VLAN Range | Mode |
|--------|------------|---------|
| Delete | | Enabled |

Add VLAN Range

Save Reset

Note: after power up, the S4224 has DHCP enabled. If a DHCP server is available, the S4224 will obtain an IP address from the DHCP server. If no DHCP server is available, after 70 seconds, the S4224 will fall back to the default IP address of 192.168.0.1/24.

The parameter entries are described below.

Global Mode

Configure operation mode to enable/disable DHCP server per system.

Mode

Configure the operation mode per system. Possible modes are:

Enabled: Enable DHCP server per system.

Disabled: Disable DHCP server per system.

VLAN Mode

Configure operation mode to enable/disable DHCP server per VLAN.

VLAN Range

Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only one VLAN ID, then you can just input it into either the first or the second VLAN ID, or both.

On the other hand, if you want to disable the existing VLAN range, then you can follow these steps.

1. Click the **Add VLAN Range** button to add a new VLAN range.
2. Enter the VLAN range that you want to disable.
3. Change the Mode to **Disabled**.
4. Click **Save** to apply the change.

The disabled VLAN range is then removed from the DHCP Server Mode Configuration page.

Mode

Indicate the operation mode per VLAN. Possible modes are:

Enabled: Enable DHCP server per VLAN.

Disabled: Disable DHCP server per VLAN.

Buttons

Add VLAN Range: Click to add a new VLAN range. You can add more than one VLAN Range per Save operation.

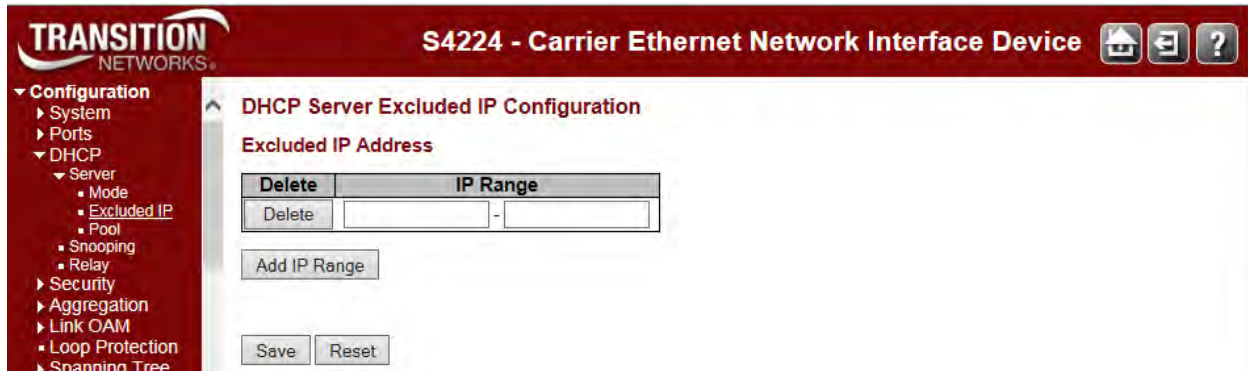
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to the previously saved values.

> DHCP Excluded IP

This page configures excluded IP addresses. The DHCP server will not allocate these excluded IP addresses to DHCP client.

Click the **Add IP Range** button to display the *DHCP Server Excluded IP Configuration* entry fields.



The excluded IP address parameters are described below.

IP Range

Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. BUT, if the IP range contains only one excluded IP, then you can just input it to either the first and second excluded IP or both.

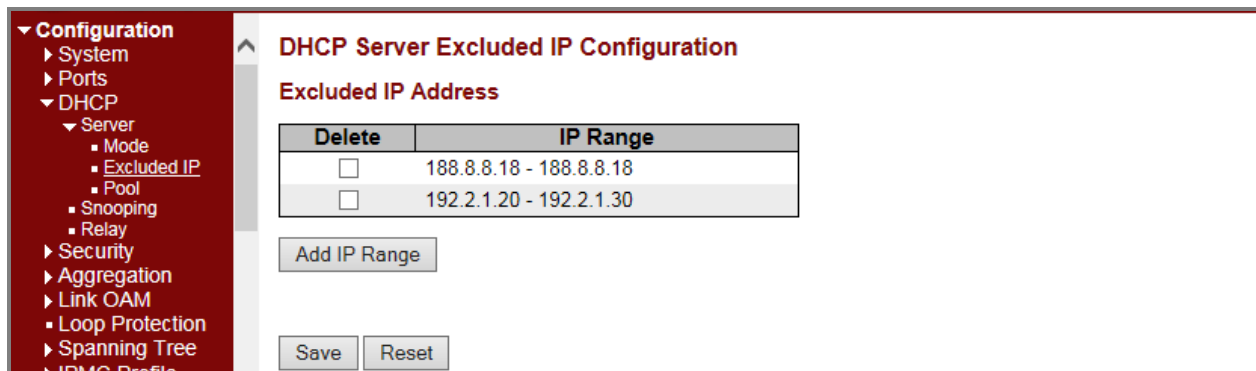
Buttons

Add IP Range: Click to add a new excluded IP range.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

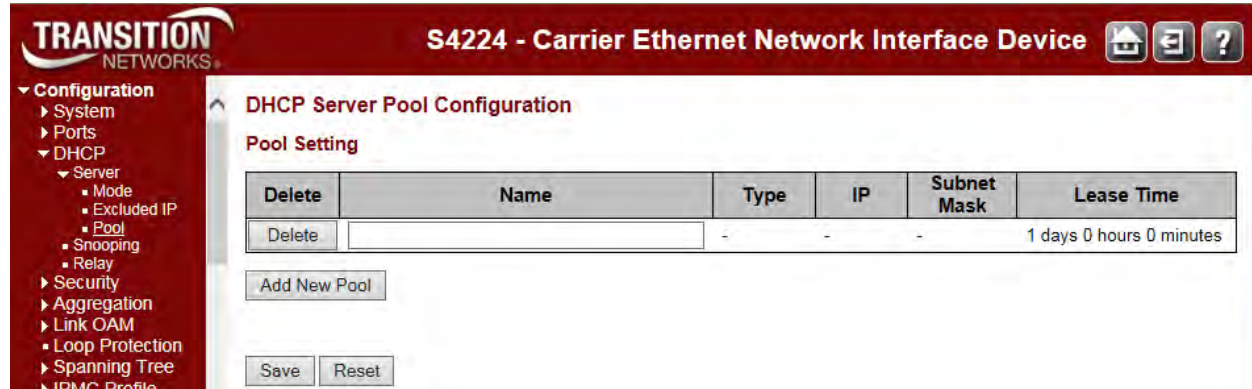
Example



> DHCP Pool

This page lets you manage DHCP pools. According to the DHCP pool, the DHCP server will allocate IP address and deliver configuration parameters to the DHCP client.

Click the **Add New Pool** button to display the entry fields.



Pool Setting

Here you can add or delete pools. Adding a pool and giving a name is to create a new pool with a "default" configuration. If you want to configure all settings including type, IP subnet mask and lease time, you can click the pool name to go into the configuration page.

Name

Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page.

Type

Display which type of the pool is.

Network: the pool defines a pool of IP addresses to service more than one DHCP client.

Host: the pool services for a specific DHCP client identified by client identifier or hardware address.

If a dash ("-") is displayed, it means not defined.

IP

Display network number of the DHCP address pool. If a dash "-" is displayed, it means not defined.

Subnet Mask

Display subnet mask of the DHCP address pool. If a dash "-" is displayed, it means not defined.

Lease Time

Displays the lease time of the pool in days hours minutes (e.g., *1 days 0 hours 0 minutes*).

Buttons

Add New Pool: Click to add a new DHCP pool.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Example

Click the linked **Name** (e.g., [DSPC100](#) below) to display the full DHCP Pool Configuration settings.

DHCP Server Pool Configuration

Pool Setting

| Delete | Name | Type | IP | Subnet Mask | Lease Time |
|--------------------------|-------------------------|------|----|-------------|--------------------------|
| <input type="checkbox"/> | DSPC100 | - | - | - | 1 days 0 hours 0 minutes |

Add New Pool

Save Reset

| | |
|-------------------------------|---------|
| Domain Name | |
| Broadcast Address | |
| Default Router | 0.0.0.0 |
| | 0.0.0.0 |
| | 0.0.0.0 |
| | 0.0.0.0 |
| DHIS Server | 0.0.0.0 |
| | 0.0.0.0 |
| | 0.0.0.0 |
| | 0.0.0.0 |
| NTP Server | 0.0.0.0 |
| | 0.0.0.0 |
| | 0.0.0.0 |
| | 0.0.0.0 |
| NetBIOS Node Type | None |
| NetBIOS Scope | |
| NetBIOS Name Server | 0.0.0.0 |
| | 0.0.0.0 |
| | 0.0.0.0 |
| | 0.0.0.0 |
| NIS Domain Name | |
| NIS Server | 0.0.0.0 |
| | 0.0.0.0 |
| | 0.0.0.0 |
| | 0.0.0.0 |
| Client Identifier | None |
| Hardware Address | |
| Client Name | |
| Vendor 1 Class Identifier | |
| Vendor 1 Specific Information | |
| Vendor 2 Class Identifier | |
| Vendor 2 Specific Information | |
| Vendor 3 Class Identifier | |
| Vendor 3 Specific Information | |
| Vendor 4 Class Identifier | |
| Vendor 4 Specific Information | |

Save Reset

The DHCP Pool Configuration parameters are described below.

Pool

Select a DHCP pool to configure the settings.

Name

Select a DHCP pool by the pool name.

Setting

Configure the DHCP pool settings.

Pool Name

Displays the selected pool name.

Type

Specify which type the pool is.

None: no pool (default).

Network: the pool defines a pool of IP addresses to service more than one DHCP client.

Host: the pool services for a specific DHCP client identified by client identifier or hardware address.

A dropdown menu with a blue border and a downward arrow on the right. The menu is open, showing three options: 'None' (highlighted in blue), 'Network', and 'Host'.

IP

Specify network number of the DHCP address pool.

Subnet Mask

DHCP option 1. Specify the subnet mask of the DHCP address pool.

Lease Time

DHCP option 51, 58 and 59. Specify a lease time that allows the client to request a lease time for the IP address. If all are 0's, then it means the lease time is infinite.

days (0-365)
hours (0-23)
minutes (0-59)

Domain Name

DHCP option 15. Specify domain name that client should use when resolving hostname via DNS.

Broadcast Address

DHCP option 28. Specify the broadcast address in use on the client's subnet.

Default Router

DHCP option 3. Specify a list of IP addresses for routers on the client's subnet.

DNS Server

DHCP option 6. Specify a list of Domain Name System name servers available to the client.

NTP Server

DHCP option 42. Specify a list of IP addresses indicating NTP servers available to the client.

NetBIOS Node Type

DHCP option 46. Specify NetBIOS node type option to allow Netbios over TCP/IP clients which are configurable to be configured as described in IETF RFC 1001/1002. This is the node type of a

networked computer which relates to the way it resolves NetBIOS names to IP addresses.

The node types are:

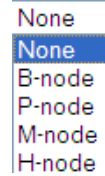
None: no node.

B-node: B- node type (0x01 Broadcast).

P-node: P- node type (0x02 Peer (WINS only)).

M-node: M- node type (0x04 Mixed (broadcast, then WINS)).

H-node: H- node type (0x08 Hybrid (WINS, then broadcast)).



The node type in use is displayed by opening a command line and typing ipconfig /all. A Windows PC registry may also be configured in such a way as to display "unknown" for the node type.

NetBIOS Scope

DHCP option 47. Specify the NetBIOS over TCP/IP scope parameter for the client as specified in IETF RFC 1001/1002.

NetBIOS Name Server

DHCP option 44. Specify a list of NBNS name servers listed in order of preference.

NIS Domain Name

DHCP option 40. Specify the name of the client's NIS (Network Information Service) domain.

NIS Server

DHCP option 41. Specify a list of IP addresses indicating NIS servers available to the client. The Network Information Service (NIS) maintains and distributes a central directory of user and group information, hostnames, e-mail aliases and other text-based tables of information in the network.

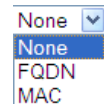
Client Identifier

DHCP option 61. Specify client's unique identifier to be used when pool is the type of host.

None: no identifier.

FQDN: fully qualified domain name (absolute domain name).

MAC: MAC identifier.



Hardware Address

Specify client's hardware (MAC) address to be used when the pool is the type of host.

Client Name

DHCP option 12. Specify the name of client to be used when the pool is the type of host.

Vendor / Class Identifier

DHCP option 60. Specify to be used by DHCP client to optionally identify the vendor type and configuration of a DHCP client. DHCP server will deliver the corresponding option 43 specific information to the client that sends option 60 vendor class identifier.

Vendor / Specific Information

DHCP option 43. Specify vendor specific information according to option 60 vendor class identifier.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Messages

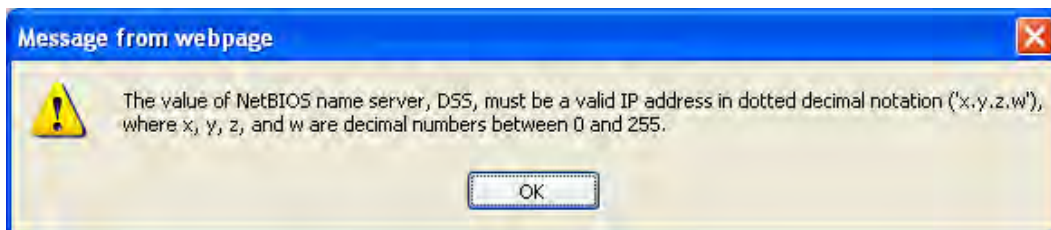
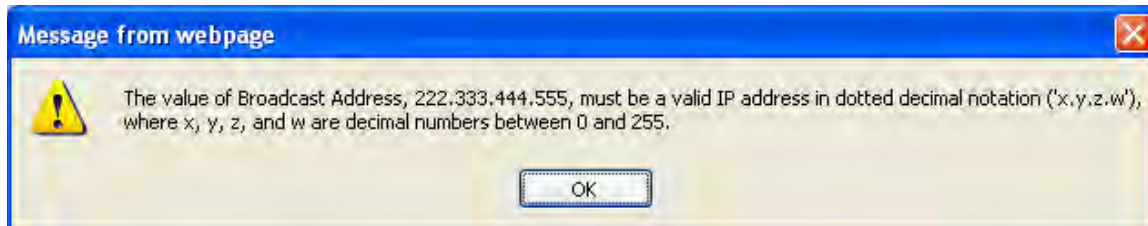
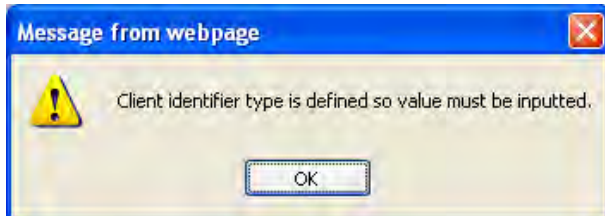
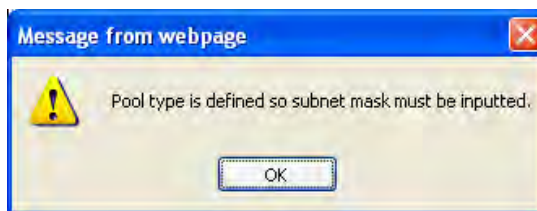
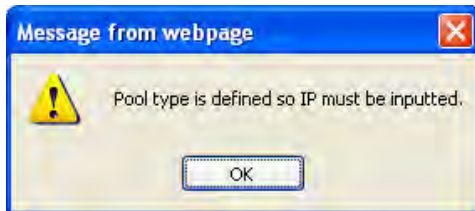
Message: Pool type is defined so IP must be inputted.

Pool type is defined so subnet mask must be inputted.

Client identifier type is defined so value must be inputted.

The value of Broadcast Address, 222.333.444.555, must be a valid IP address in dotted decimal notation ("x.y.z.w"), where x, y, z, and w are decimal numbers between 0 and 255.

The value of NetBIOS name server, DSS, must be a valid IP address in dotted decimal notation ("x.y.z.w"), where x, y, z, and w are decimal numbers between 0 and 255.

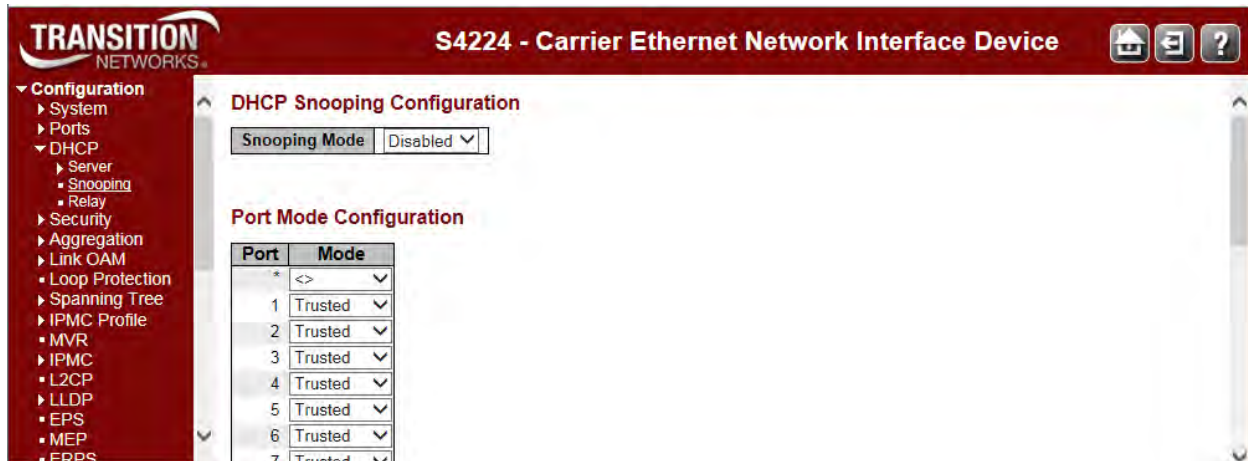


Meaning: A DHCP parameter was configured incorrectly.

Recovery: 1) Click the **OK** button to clear the webpage message. 2) Re-enter the parameter correctly. See the preceding section for details.

Configuration > DHCP > DHCP Snooping

Configure DHCP Snooping on this page. DHCP Snooping is used to block an intruder on the untrusted switch ports when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.



The DHCP Snooping parameters are described below.

DHCP Snooping Mode

Indicates the DHCP snooping mode operation. Possible modes are:

Enabled: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

Disabled: Disable DHCP snooping mode operation.

Port Mode Configuration

Indicates the DHCP snooping port mode. Possible port modes are:

Trusted: Configures the port as trusted source of the DHCP messages.

Untrusted: Configures the port as untrusted source of the DHCP messages.

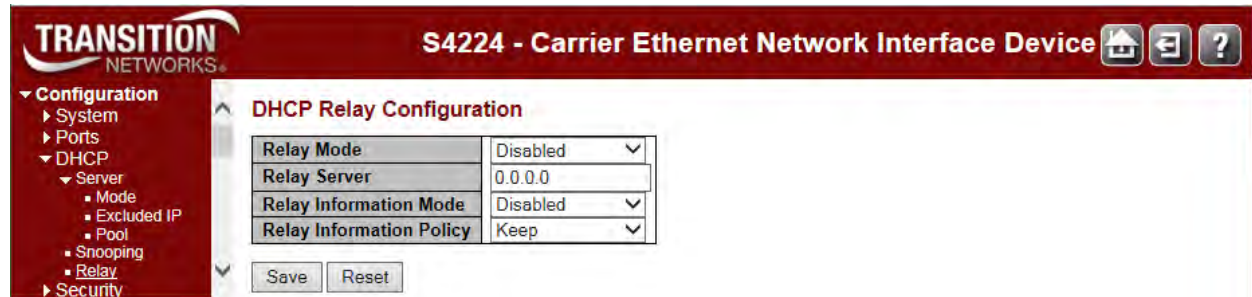
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Configuration > DHCP > DHCP Relay

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such condition, please make sure the switch configuration of VLAN interface IP address and PVID (Port VLAN ID) correctly.



Relay Mode

Indicates the DHCP relay mode operation. Possible modes are:

Enabled: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.

Disabled: Disable DHCP relay mode operation.

Relay Server

Indicates the DHCP relay server IP address.

Relay Information Mode

Indicates the DHCP relay information mode option operation. The option 82 circuit ID format is "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (in standalone device it always equal 0, in a stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message received from VLAN ID 3, switch ID 1, port No 8. The option 82 remote ID value is equal to the switch MAC address. Valid modes are:

Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.

Disabled: Disable DHCP relay information mode operation.

Relay Information Policy

Indicates the DHCP relay information option policy. When DHCP relay information mode is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:

Replace: Replace the original relay information when a DHCP message that already contains it is received.

Keep: Keep the original relay information when a DHCP message that already contains it is received.

Drop: Drop the package when a DHCP message that already contains relay information is received.

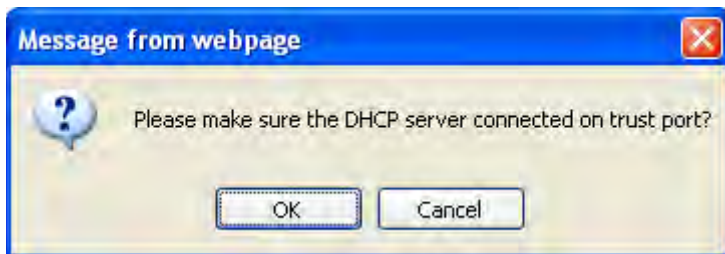
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Messages

Message: Please make sure the DHCP server connected on trust port?



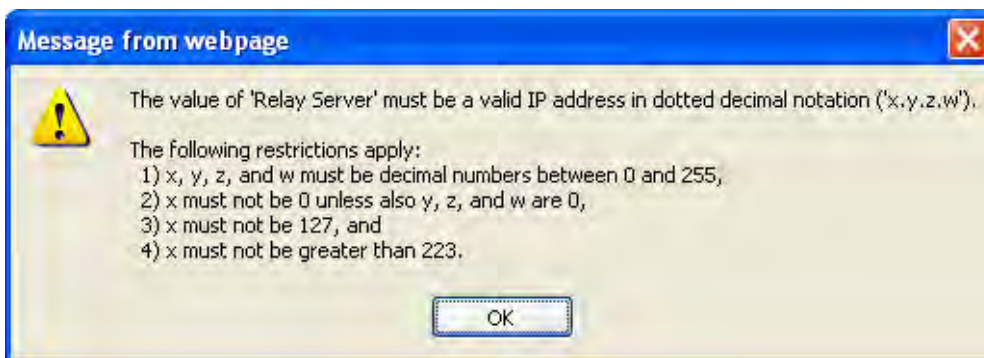
Meaning: A warning message to make sure that the DHCP Server is connected on a port that is configured as “trusted”.

Recovery: 1) Click the **OK** button to clear the webpage message. 2) Verify the parameter entry. See the preceding section for details.

Message: The value of 'Relay server' must be a valid IP address in dotted decimal notation ('x.y.z.w').

The following restrictions apply:

- 1) x, y, z, and w must be decimal numbers between 0 and 255,
- 2) x must not be 0 unless also y, z, and w are 0,
- 3) x must not be 127, and
- 4) x must not be greater than 223.



Meaning: A DHCP parameter was configured incorrectly.

Recovery: 1) Click the **OK** button to clear the webpage message. 2) Re-enter the parameter correctly. See the preceding section for details.

S4224 DHCP Configuration Process

Notes:

1. Software releases supporting DHCP Server: S3290 v 2.1.x and S42240, S4140 v 2.2.x.
2. To configure DHCP server you must have a VLAN interface setup with a valid IP address.
3. DHCP Server does not support addresses that come from a DHCP relay server. It must directly handle relay packets.
4. May have to turn off some DHCP options in the DHCP client. See "DHCP Options Used" below.
5. DHCP works the same on 1G ports as on 10G ports.
6. S3290 DHCP supports multiple DHCP Pools (one Pool for each VLAN on multiple ports).
7. S3290 DHCP supports multiple Pools/VLANs serving addresses on a single port.

A. At Configuration > System > IP

DHCP clients require the S3290 to have a VLAN interface for the VLAN with a statically configured IP address before the S3290 will assign IP addresses on that port. *This step does not necessarily need to be completed before the next step, but it is recommended from a configuration perspective (i.e., if any other VLAN configurations are to be completed).*

1. Set up IP Configuration at **Configuration > System > IP**:
 - a. Configure IP Address and sub VLAN IDs for the VLANs that will serve the DHCP assigned IP Address.
 - b. Choose either '**Router**' mode or '**Host**' mode and save. **Router** mode forwards traffic between interfaces; it may make things more complicated if there are other DHCP servers on the network.
2. Set up IP Interfaces at **Configuration > System > IP**:
 - a. Click the **Add Interface** button.
 - b. Configure the Allowed VLAN range.

B. At Configuration > DHCP

3. Configure DHCP Server:
 - a. Enable Global Mode; click the **Add VLAN Range** button and configure VLAN Mode.
4. Configure Pool Setting. Add a DHCP Address Pool at **Configuration > DHCP > Server > Pool**:
 - a. Add a Name and save the Pool entry.
 - b. Configure Type as 'Host' or 'Network'. **Network**: the pool defines a pool of IP addresses to service more than one DHCP client. **Host**: the pool services for a specific DHCP client identified by client identifier or hardware address.
 - c. Configure the IP Address corresponding to the VLAN ID that will serve the addresses. This will correspond to the IP address you configured at **Configuration > System > IP** in step 1a above. (**Note**: for 'Network' Type, this will be a network address with an associated subnet mask. All clients will take on the subnet mask configured.)
Note: The IP address here should not be the router IP address unless you are in 'Host' mode and the host you are configuring is the router.
 - d. Configure a subnet mask.
 - e. Configure the Lease time in days.
 - f. Configure the broadcast address. For example, for an address of 10.0.1.1/24 the notation would be 10.0.1.255.
 - g. Configure the default router. This will be the IP address entered as 'Host' in step 4b above.
 - h. Enter any additional configuration needed for the DHCP Setup and save.
5. Configure DHCP Snooping: enable Snooping Mode and configure Port Modes as required.

7. Configure DHCP Options: set DHCP Forwarding Configuration as required.

8. Once the server has been configured check **Monitor > DHCP** pages for activity on the server. The counters under the Statistics page and the Bindings page allow you to click on each IP address the server has handed out and view its associated MAC address.

Web Interface Screen Examples

A. Configuration > System > IP

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

IP Configuration

| | |
|--------------|--------------------------|
| Mode | Host |
| DNS Server 0 | No DNS server |
| DNS Server 1 | No DNS server |
| DNS Server 2 | No DNS server |
| DNS Server 3 | No DNS server |
| DNS Proxy | <input type="checkbox"/> |

IP Interfaces

| Delete | VLAN | DHCPv4 | | | IPv4 | | DHCPv6 | | | IPv6 | |
|--------------------------|------|--------------------------|----------|---------------|--------------|-------------|--------------------------|--------------------------|---------------|---------|-------------|
| | | Enable | Fallback | Current Lease | Address | Mask Length | Enable | Rapid Commit | Current Lease | Address | Mask Length |
| <input type="checkbox"/> | 1 | <input type="checkbox"/> | 0 | | 192.168.1.11 | 24 | <input type="checkbox"/> | <input type="checkbox"/> | | | |

Add Interface

IP Routes

| Delete | Network | Mask Length | Gateway | Next Hop VLAN |
|--------------------------|---------|-------------|---------|---------------|
| <input type="checkbox"/> | | | | |

Add Route

Save Reset

B. Configuration > DHCP > Server > Mode

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

DHCP Server Mode Configuration

Global Mode

Mode: Enabled

VLAN Mode

| Delete | VLAN Range | Mode |
|--------------------------|------------|---------|
| <input type="checkbox"/> | 100 - 301 | Enabled |

Add VLAN Range

Save Reset

B. Configuration > DHCP > Server > Pool

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

Configuration

- System
- Ports
- DHCP
 - Server
 - Mode
 - Excluded IP
 - Pool
 - Snooping
 - Relay
 - Options
 - Security
 - Aggregation
 - Link OAM
 - Loop Protection
 - Spanning Tree

DHCP Server Pool Configuration

Pool Setting

| Delete | Name | Type | IP | Subnet Mask | Lease Time |
|--------------------------|--------|---------|---------------|---------------|--------------------------|
| <input type="checkbox"/> | dPool1 | Network | 192.168.1.200 | 255.255.255.0 | 1 days 0 hours 0 minutes |

Buttons: Add New Pool, Save, Reset

B. Configuration > DHCP > Server > Pool

Click on linked Pool Name once added.

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

Configuration

- System
- Ports
- DHCP
 - Server
 - Mode
 - Excluded IP
 - Pool
 - Snooping
 - Relay
 - Options
 - Security
 - Aggregation
 - Link OAM
 - Loop Protection
 - Spanning Tree
 - IPMC Profile
 - MTR
 - IPMC
 - L2DP
 - LLDP
 - ERPS
 - MEP
 - ERPS
 - MAC Table
 - VLAN Translation
 - VLANs
 - Private VLANs
 - VCL
 - Ethernet Services
 - Performance Monitor
 - QoS
 - Mirroring
 - PTP
 - GVRP
 - Service Activation
 - DDMI
 - UCLD
- Monitor
- Diagnostics
- Maintenance

DHCP Pool Configuration

Pool Name: dPool1

Setting

| | |
|-------------------------------|--|
| Pool Name | dPool1 |
| Type | Network |
| IP | 192.168.1.200 |
| Subnet Mask | 255.255.255.0 |
| Lease Time | 1 days (0-365) 0 hours (0-23) 0 minutes (0-59) |
| Domain Name | |
| Broadcast Address | 0.0.0.0 |
| Default Router | 0.0.0.0 |
| DNS Server | 0.0.0.0 |
| NTP Server | 0.0.0.0 |
| NetBIOS Node Type | None |
| NetBIOS Scope | 0.0.0.0 |
| NetBIOS Name Server | 0.0.0.0 |
| NIS Domain Name | 0.0.0.0 |
| NIS Server | 0.0.0.0 |
| Client Identifier | None |
| Hardware Address | |
| Client Name | |
| Vendor 1 Class Identifier | |
| Vendor 1 Specific Information | |
| Vendor 2 Class Identifier | |
| Vendor 2 Specific Information | |
| Vendor 3 Class Identifier | |
| Vendor 3 Specific Information | |
| Vendor 4 Class Identifier | |
| Vendor 4 Specific Information | |

Buttons: Save, Reset

Additional Notes

1. The IP address in step B/C should not be the router unless you are in host mode" and the host you are configuring is the router. In network mode, the IP address in B/C should not be an IP address but a network address (192.168.99.0 in my example). The Default Router IP address should be the IP address of the router on that network. This could be the VLAN interface on the DHCP server or an actual router plugged into the DHCP server.
2. Re: Note 4 on page 1: If a packet DHCP packet has been relayed before it gets to our DHCP server, our DHCP server will drop it. The workaround is to not use a relay and run a DHCP server on the device you want to run a relay on.
3. Some Linux clients enable RFC 4361 (DUID) support by default. You may have to have these Linux clients revert to RFC 2131/2132 (ClientID) in order to work. DUID (DHCP Unique Identifier) is a way to send a unique ID for both IPv4 and IPv6 clients to a DHCP server. ClientID is a simpler unique ID for IPv4 only.
4. Configuring DHCP Relay is not supported (Relay Mode and Server, Info Mode, and Info Policy).
5. The maximum number of Pools/addresses that can be served per Port depends on available memory on the device, so simpler setups can handle more IP addresses; devices with more memory can handle more IP addresses (the S3290 has 82MB; the S4224 has 73MB).

DHCP Options Used

See the IANA web site at <http://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml> for more DHCP options information. See the IETF web site for RFC 2132 information at <http://tools.ietf.org/html/rfc2132> and at <http://www.networksorcery.com/enp/rfc/rfc4361.txt> for RFC 4361 information.

Subnet Mask: DHCP option 1. Specify subnet mask of the DHCP address pool.

Lease Time: DHCP option **51**, **58** and **59**. Specify lease time that allows the client to request a lease time for the IP address. If all are 0's, then it means the lease time is infinite.

Domain Name: DHCP option **15**. Specify domain name that client should use when resolving hostname via DNS.

Broadcast Address: DHCP option **28**. Specify the broadcast address in use on the client's subnet.

Default Router: DHCP option **3**. Specify a list of IP addresses for routers on the client's subnet.

DNS Server: DHCP option **6**. Specify a list of Domain Name System name servers available to the client.

NTP Server: DHCP option **42**. Specify a list of IP addresses indicating NTP servers available to the client.

NetBIOS Node Type: DHCP option **46**. Specify NetBIOS node type option to allow Netbios over TCP/IP clients which are configurable to be configured as described in RFC 1001/1002.

NetBIOS Scope: DHCP option **47**. Specify the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002.

NetBIOS Name Server: DHCP option **44**. Specify a list of NBNS name servers listed in order of preference.

NIS Domain Name: DHCP option **40**. Specify the name of the client's NIS domain.

NIS Server: DHCP option **41**. Specify a list of IP addresses indicating NIS servers available to the client.

Client Identifier: DHCP option **61**. Specify client's unique identifier to be used when the pool is the type of host.

Client Name: DHCP option **12**. Specify the name of client to be used when the pool is the type of host.

Vendor i Class Identifier: DHCP option **60**. Specify to be used by DHCP client to optionally identify the vendor type and configuration of a DHCP client. DHCP server will deliver the corresponding option 43 specific information to the client that sends option 60 vendor class identifier.

Vendor i Specific Information: DHCP option **43**. Specify vendor specific information according to option 60 vendor class identifier.

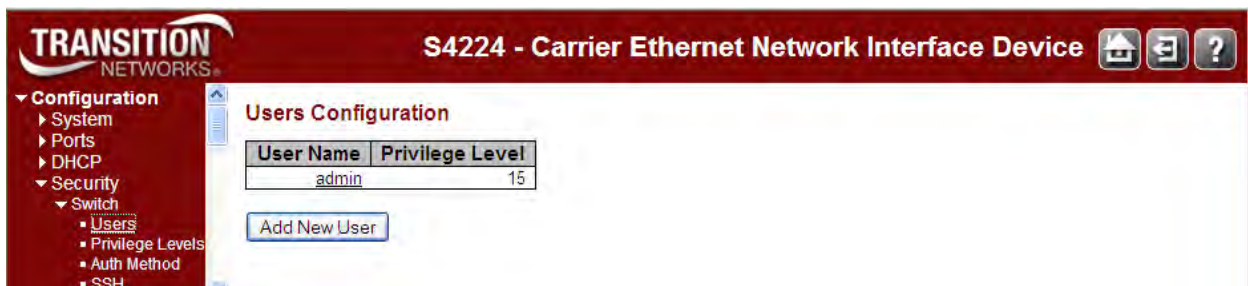
System Users Configuration

Configuration > Security > Switch > Users

The **Configuration > Security > Switch > Users** menu path lets you view and configure the system users that are allowed to access the web pages or log in from CLI.

You can also access the S4224 System Password page from the **Configuration > Security > Switch > Users** menu path.

This page provides an overview of the currently defined system users. Currently the only way to login as another user on the web server is to close and reopen the browser.



User Name

Enter the new user's name to be added (the name identifying the user). This is also a link to Add, Edit or Delete an existing User.

Privilege Level

Enter the new user's level of access to be allowed. This is the privilege level of the user. The valid range is **1** - **15**.

If the privilege level value is **15**, a user can access all groups (i.e., this user is granted the fully control of the device). But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group.

The system maintenance (software upload, factory defaults and etc.) requires user privilege level 15. By default, most groups' privilege level **5** has read-only access and privilege level **10** has read-write access. Generally, privilege level **15** can be used for an administrator account, privilege level **10** for a standard user account, and privilege level **5** for a guest account.

Buttons

Add New User: Click to add a new user to the Users Configuration table.

Edit User (Edit the Default admin User)

To edit the default admin user, click the admin link to display the Edit User page. This page lets you configure the system password required to access the web pages or log in from CLI.

| User Settings | |
|------------------|-------|
| User Name | admin |
| Password | |
| Password (again) | |
| Privilege Level | 15 |

Save Reset Cancel

Enter the **Password** and **Privilege Level** as described below.

Add a New User

To add a new user, click the Add New **user** button. The **Add User** table displays.

| User Settings | |
|------------------|---|
| User Name | |
| Password | |
| Password (again) | |
| Privilege Level | 1 |

Save Reset Cancel

The parameters are explained below.

User Name

A string identifying the user name that this entry should belong to. The allowed string length is **1** to **32**. A valid user name can include a combination of letters, numbers and underscores.

Password

The password of the user. The allowed string length is **0** to **32** alpha, numeric, or special characters.

Password (again)

Enter the Password again to confirm. These entries must match exactly.

The new password must be entered twice to catch typing errors. The message "*Password Error - The old password is incorrect. New password is not set.*" displays if the new password entered is the same as the old password. If this occurs, click the browser Back button and enter a unique new password and confirm with an identical entry.

Privilege Level

The privilege level of the user. The allowed range is **1** to **15**. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values may be needed to refer to each group privilege level. A User's privilege level should be same or greater than the Group privilege level to have the access of that group.

In general, the user privilege levels are:

Privilege Level 15 can be used for an Administrator account. Privilege level 15 allows system Maintenance menu access (software upload, factory defaults, etc.).

Privilege Level 10 for a Standard (basic) user account. Privilege level 10 allows read-write access.

Privilege Level 5 for a Guest account. By default, most groups privilege are assigned privilege level 5 (read-only access).

See the "Privilege Level Configuration" section below for more information.

Buttons

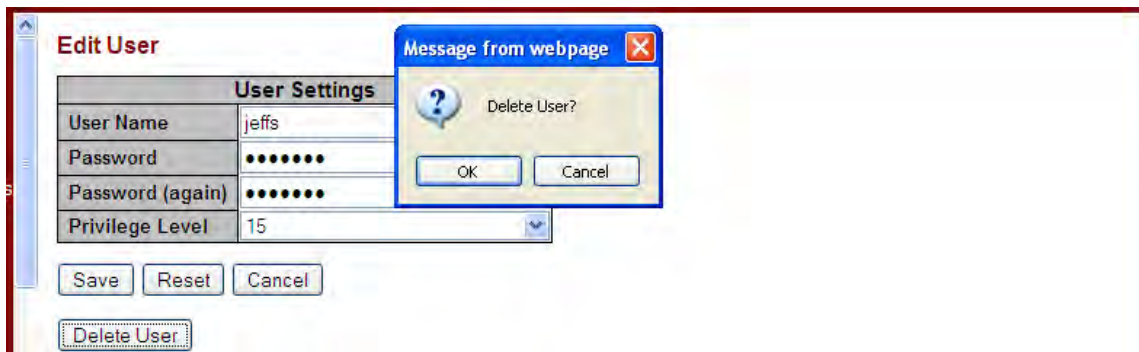
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Click to undo any changes made locally and return to the Users.

Delete an Existing User

To delete an existing user from the table, click the user's name to be deleted. The Edit User table displays.



Click the **Delete User** button. At the confirmation webpage message (*Delete User?*), click the **OK** button.

The Users Configuration table re-displays without the deleted user.

Privilege Levels Configuration

Configuration ->Security > Switch > Privilege Levels

This page lets you view and edit users' privilege (access) levels from the **Configuration ->Security > Switch > Privilege Levels** menu path. **Note:** this feature only works for web users.

- ▼ Configuration
 - ▶ System
 - ▶ Ports
 - ▶ DHCP
 - ▼ Security
 - ▼ Switch
 - Users
 - **Privilege Levels**
 - Auth Method
 - SSH
 - HTTPS
 - Access Management
 - ▶ SNMP
 - ▶ RMON
 - ▶ Network
 - ▶ AAA
 - ▶ Aggregation
 - ▶ Link OAM
 - Loop Protection
 - ▶ Spanning Tree
 - ▶ IPMC Profile
 - MVR
 - ▶ IPMC
 - L2CP
 - ▶ LLDP
 - SyncE
 - EPS
 - MEP
 - ERPS
 - MAC Table
 - ▶ VLAN Translation
 - VLANs
 - ▶ Private VLANs
 - ▶ VCL
 - ▶ Ethernet Services
 - ▶ Performance Monitor
 - ▶ QoS
 - Mirroring
 - PTP
 - ▶ GVRP
 - ▶ Service Activation
 - ▶ DDMI
 - UDLD
 - ▶ Monitor
 - ▶ Diagnostics
 - ▶ Maintenance

Privilege Level Configuration

| Group Name | Privilege Levels | | | |
|---------------------|-------------------------|----------------------------------|-----------------------------|------------------------------|
| | Configuration Read-only | Configuration/Execute Read/write | Status/Statistics Read-only | Status/Statistics Read/write |
| Aggregation | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| DDMI | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| Debug | 15 ▼ | 15 ▼ | 15 ▼ | 15 ▼ |
| DHCP | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| DHCPv6_Client | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| Diagnostics | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| EPS | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| ERPS | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| ETH_LINK_OAM | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| ETHER_SAT | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| EVC | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| IP | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| IPMC_Snooping | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| LACP | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| LLDP | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| Loop_Protect | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| MAC_Table | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| Maintenance | 15 ▼ | 15 ▼ | 15 ▼ | 15 ▼ |
| MEP | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| MVR | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| NTP | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| Performance_Monitor | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| Ports | 5 ▼ | 10 ▼ | 1 ▼ | 10 ▼ |
| Private_VLANs | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| PTP | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| QoS | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| RMirror | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| Security | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| Spanning_Tree | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| System | 5 ▼ | 10 ▼ | 1 ▼ | 10 ▼ |
| UDLD | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| VCL | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| VLAN_Translation | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| VLANs | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |
| XXRP | 5 ▼ | 10 ▼ | 5 ▼ | 10 ▼ |

The **Group Name** column lists the S4224 main functions, including Aggregation, DDMI, Debug, DHCP, DHCPv6_Client, Diagnostics, EPS, ERPS, ETH_LINK_OAM, EtherSAT, EVC, IP, IPMC_Snooping, LACP, LLDP, Loop_Protect, MAC_Table, Maintenance, MEP, MVR, NTP, Performance_Monitor, Ports, Private_VLANs, PTP, QoS, RMirror, Security, Spanning_Tree, System, UDLD, VCL, VLAN_Translation, VLANs, and XXRP.

The Privilege Level parameters are explained below.

Group Name

The name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but some groups contain more than one module.

Some of these privilege level groups are explained below.

System: e.g., Contact, Name, Location, Timezone, Log.

Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and IP source guard.

IP: Everything except 'ping'.

Port: Everything except 'VeriPHY'.

Diagnostics: 'ping' and 'VeriPHY'.

Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance. Debug is only present in the CLI.

Privilege Levels

Every group has an authorization Privilege level for the following sub groups: Configuration read-only, Configuration/execute read-write, Status/statistics read-only, Status/statistics read-write (e.g., for clearing statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

Configuration read-only: these users are only allowed to monitor status / configuration settings.

Configuration/execute read-write: these users are only allowed to monitor status and make changes to configuration settings.

Status/statistics read-only: these users are only allowed to monitor status / statistics settings. The privilege level of 'Read-only' should be less or equal 'Read/Write'.

Status/statistics read-write: (e.g., for clearing statistics).

User Privilege Levels (1-15)

The privilege level of the user. The allowed range is **1** to **15**.

Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics).

If the privilege level value is 15, it can access all groups (i.e. it is granted full control of the device). But other values need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level in order to have the access of that group. By default, most groups have privilege level 5 with read-only access; privilege level 10 has the read-write access. The system maintenance functions (software upload, factory defaults, etc.) require user privilege level 15.

Generally, the user privilege levels are:

Privilege Level 15 can be used for an Administrator account,

Privilege Level 10 is for a Standard (basic) user account, and

Privilege Level 5 is for a Guest account.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Message: *Must explicitly add case for module ID: %d*

Meaning: A user privilege level was not defined for a module.

Recovery: 1. Define a privilege level for the module (e.g., crw = 10).

Authentication Method Configuration

Configuration > Security > Switch > Auth Method

The authentication section allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces. Access this page from the **Configuration > Security > Switch > Auth Method** menu path.

Authentication Method Configuration

| Client | Method | no | no |
|---------|--------|----|----|
| console | local | no | no |
| telnet | local | no | no |
| ssh | local | no | no |
| http | local | no | no |

Command Authorization Method Configuration

| Client | Method | Cmd Lvl | Cfg Cmd |
|---------|--------|---------|--------------------------|
| console | no | 0 | <input type="checkbox"/> |
| telnet | no | 0 | <input type="checkbox"/> |
| ssh | no | 0 | <input type="checkbox"/> |

Accounting Method Configuration

| Client | Method | Cmd Lvl | Exec |
|---------|--------|---------|--------------------------|
| console | no | | <input type="checkbox"/> |
| telnet | no | | <input type="checkbox"/> |
| ssh | no | | <input type="checkbox"/> |

Save Reset

Authentication Method Configuration

The authentication section allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces. The table has one row for each client type and a number of columns, which are:

Client

The management client for which the configuration below applies (console, telnet, ssh, or http).

Methods

Method can be set to one of the following values:

no: Authentication is disabled and login is not possible.

local: Use the local user database on the switch for authentication.

radius: Use remote RADIUS server(s) for authentication. **Remote Authentication Dial In User Service** is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

tacacs: Use remote TACACS+ server(s) for authentication. **Terminal Access Controller Access Control System Plus**. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Authentication Method Configuration

| Client | Method | no | no |
|---------|--------|--------|----|
| console | local | no | no |
| telnet | radius | no | no |
| ssh | tacacs | no | no |
| http | local | local | no |
| | | radius | |
| | | tacacs | |

Save Reset

Methods that involve remote servers are timed out if the remote servers are offline. In this case, the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for 'primary' authentication, it is recommended to configure secondary authentication as 'local'. This lets the management client login via the local user database if none of the configured authentication servers are alive.

Well known ports: TACACS+ uses port # 49. RADIUS Authentication uses port # 1812. RADIUS Accounting uses port # 1812.

Command Authorization Method Configuration

The command authorization section allows you to limit the CLI commands available to a user. **Note:** this feature is currently not fully functional. The table has one row for each client type and a number of columns, which are:

Client

The management client for which the configuration below applies.

Method

Method can be set to one of the following values:

no: Command authorization is disabled. User is granted access to CLI commands according to his privilege level.

tacacs: Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.

Cmd Lvl

Authorize all commands with a privilege level higher than or equal to this level. Valid values are in the range **0** to **15**.

Cfg Cmd

Check to also authorize configuration commands.

Accounting Method Configuration

The accounting section allows you to configure logging of all CLI command and exec (login) to an *accounting.log* file on the TACACS+ server. The table has one row for each client type (console, telnet, and ssh) and a number of columns, as described below:

Client

The management client for which the configuration below applies.

Method

Method can be set to one of the following values:

no: Accounting is disabled.

tacacs: Use remote TACACS+ server(s) for accounting.

Cmd Lvl

Enable logging of all CLI commands with a privilege level higher than or equal to this level. Valid values are **0** - **15**. Leave the field empty to disable command accounting.

Exec

Enable exec (login) accounting to the TACACS+ server.

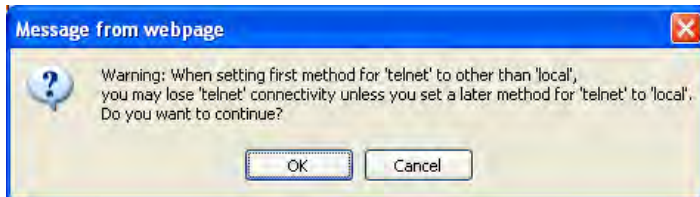
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Messages

Warning: When setting first method for 'telnet' to other than 'local', you may lose 'telnet' connectivity unless you set a later method for 'telnet' to 'local'. Do you want to continue?



Problem: With TACACS+ accounting enabled, the command privilege level filtering option does not always work as expected. At the default level of 0, all commands are logged as expected. After setting the level to 1, which should log commands level 1 and above, some level 5 commands are not logged. This includes, but is not limited to, "Show IP", "Show Clock", and "Show System". Other level 5 commands such as "Show SNMP" and "Show Spanning Tree" continue to be logged even after the filter is set above level 5.

Workaround: This problem does not effect the ability to log commands; a work around is to edit/filter the accounting log on the TACACS server.

Examples

Below is a sample log of all CLI commands from: a TACACS+ accounting log from the TACACS server:

```

accounting.log - Notepad
File Edit Format View Help
wed Jun 24 13:29:13 2015 192.251.180.40 admin console <none> stop task_id=92 service=shell cmd=logout
wed Jun 24 13:29:21 2015 192.251.180.40 admin console <none> stop task_id=93 service=shell cmd=configure
terminal
wed Jun 24 13:29:38 2015 192.251.180.40 admin console <none> stop task_id=93 service=shell cmd=monitor
session 1
wed Jun 24 13:30:22 2015 192.251.180.40 admin console <none> stop task_id=93 service=shell cmd=logging
wed Jun 24 13:30:26 2015 192.251.180.40 admin console <none> stop task_id=93 service=shell cmd=logging
wed Jun 24 13:30:32 2015 192.251.180.40 admin console <none> stop task_id=93 service=shell cmd=endwed
Jun 24 13:30:36 2015 192.251.180.40 admin console <none> stop task_id=93 service=shell cmd=logout
wed Jun 24 13:30:36 2015 192.251.180.40 admin console <none> stop task_id=93 service=shell cmd=
wed Jun 24 13:30:39 2015 192.251.180.40 admin console <none> start task_id=94 service=shell cmd=wed Jun
24 13:30:42 2015 192.251.180.40 admin console <none> stop task_id=94 service=shell cmd=configure
terminal
wed Jun 24 13:30:54 2015 192.251.180.40 admin console <none> stop task_id=94 service=shell cmd=vlan
wed Jun 24 13:31:26 2015 192.251.180.40 admin console <none> stop task_id=94 service=shell cmd=vlan
protocol snap 0 15
wed Jun 24 13:31:38 2015 192.251.180.40 admin console <none> stop task_id=94 service=shell cmd=vlan
protocol snap 0 15 group
wed Jun 24 13:31:49 2015 192.251.180.40 admin console <none> stop task_id=94 service=shell cmd=vlan
protocol snap 0 15 group o
wed Jun 24 13:33:06 2015 192.251.180.40 admin telnet 192.251.180.6 start task_id=95 service=shell cmd=
wed Jun 24 13:33:15 2015 192.251.180.40 admin telnet 192.251.180.6 stop task_id=95 service=shell

```

A sample Auth Method config screen is shown below: Note that AAA is also configurable from the **Configuration > Security > AAA > TACACS+** menu path.

The screenshot shows the web interface for a Transition Networks S4224 Carrier Ethernet Network Interface Device. The left sidebar contains a navigation menu with categories like Configuration, System, Ports, DHCP, Security, Switch, Users, Privilege Levels, Auth Method, SSH, HTTPS, Access, Management, SNMP, RMON, Network, AAA, Aggregation, Link OAM, Loop Protection, Spanning Tree, IPMC Profile, MVR, IPMC, L2CP, LLDP, SyncE, EPS, MEP, ERPS, and MAC Table. The main content area is titled 'Authentication Method Configuration' and contains three tables: 'Authentication Method Configuration', 'Command Authorization Method Configuration', and 'Accounting Method Configuration'. At the bottom of the main area are 'Save' and 'Reset' buttons.

Authentication Method Configuration

| Client | Methods | | |
|---------|---------|--------|-------|
| console | local | no | no |
| telnet | radius | tacacs | local |
| ssh | tacacs | radius | local |
| http | local | no | no |

Command Authorization Method Configuration

| Client | Method | Cmd Lvl | Cfg Cmd |
|---------|--------|---------|-------------------------------------|
| console | no | 10 | <input checked="" type="checkbox"/> |
| telnet | tacacs | 10 | <input checked="" type="checkbox"/> |
| ssh | tacacs | 10 | <input checked="" type="checkbox"/> |

Accounting Method Configuration

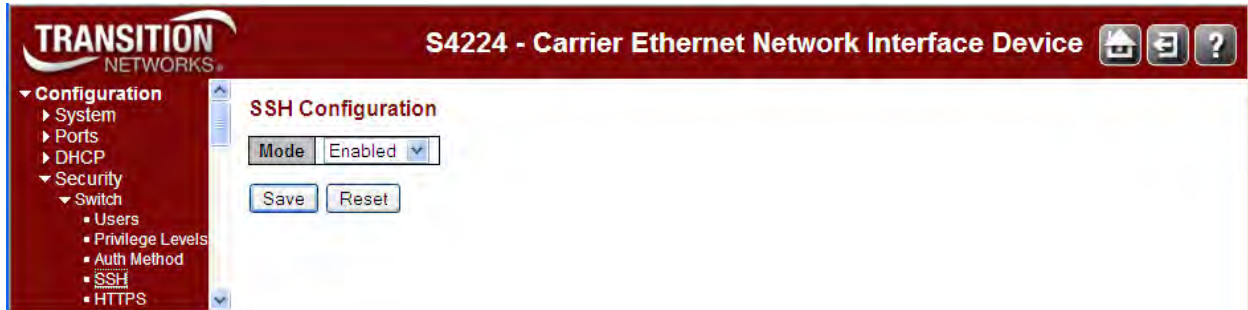
| Client | Method | Cmd Lvl | Exec |
|---------|--------|---------|-------------------------------------|
| console | no | 15 | <input checked="" type="checkbox"/> |
| telnet | tacacs | 15 | <input checked="" type="checkbox"/> |
| ssh | tacacs | 15 | <input checked="" type="checkbox"/> |

Save Reset

SSH Configuration

Configure SSH on this page from the **Configuration - Security - Switch - SSH** menu path.

The SSH (Secure Shell) network protocol allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality.



The SSH parameter:

Mode

Indicates the SSH mode operation. Possible modes are:

Enabled: Enable SSH mode operation (the default mode).

Disabled: Disable SSH mode operation.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

HTTPS Configuration

Configure HTTPS on this page from the **Configuration - Security - Switch - HTTPS** menu path. Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is used to indicate a secure HTTP connection. HTTPS provides authentication and encrypted communication.

The S4224 has an embedded web server for managing the device without any additional software. The web server also provides a secure interface using HTTPS. The validity period will be based on the validity period of the uploaded cert. If using a generated cert, then the HTTPS Certificate's validity period is from Jan. 1, 2010 to Dec. 31, 2029.

By default the servers listen on standard port 80 for HTTP and on standard port 443 for HTTPS. The HTTPS runs over SSL and the certificate can be uploaded by the user using standard TFTP protocol. You can reconfigure the HTTPS server port for security purposes. No password is used for the SSH certificate. Open SSL commands are available for self-signing a certificate.



Mode

Indicates / sets the HTTPS mode operation. The possible modes are:

Enabled: Enable HTTPS mode operation. After a change from 'Disabled' to 'Enabled' and a 'Save', you must login in secure mode (i.e., from <https://192.168.1.110>).

Disabled: Disable HTTPS mode operation. After a change from 'Enabled' to 'Disabled' and a 'Save', you must login in non-secure mode (i.e., from <http://192.168.1.110>).

Automatic Redirect

Indicates the HTTPS redirect mode operation. Automatically redirect web browser to HTTPS when HTTPS mode is enabled. Possible modes are:

Enabled: Enable HTTPS redirect mode operation.

Disabled: Disable HTTPS redirect mode operation. Note: You can not enable the HTTPS redirect function when the HTTPS operation mode is disabled.

The valid HTTPS configurations are:

Mode = Disabled and **Automatic Redirect** = Disabled, or

Mode = Enabled and **Automatic Redirect** = Disabled, or

Mode = Enabled and **Automatic Redirect** = Enabled.

If you enable both "Mode" and "Automatic Redirect", these messages display: "Content was blocked because it was not signed by a valid security certificate." and "There is a problem with this website's security certificate.". Select "Continue to this website (not recommended)". At the login dialog box, enter the login information. The startup screen ("Port State Overview") displays from the new (secure) login IP address (e.g., <https://192.168.1.110/>).

Certificate Maintain

This field only can be configured when HTTPS is disabled. It is used to maintain the certification. Possible actions are:

None: No action for certification.

Delete: To delete a certification.

Upload: To upload a certification, there are two kind of upload method can be selected: Web Browser or URL.

Generate: To generate certification.

Certificate Algorithm

HTTPS can generate two types of certification. Possible types are:

RSA: generate an RSA key. Uses the RSA internet encryption and authentication system via an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman.

DSA: generate a DSA key. Uses the digital signature algorithm (DSA) developed by the U.S. National Security Agency (NSA) to generate a digital signature for the authentication of electronic documents. Digital signatures are generated and verified via DSA. Signatures are generated in conjunction with the use of a private key; verification takes place in reference to a corresponding public key.

PassPhrase

The pattern is used for encrypting the certification.

Certificate Upload

Possible modes are:

Web Browser: To Upload certification via the Web browser.

URL: To Upload certification via URL; the supported protocols are HTTP, TFTP and FTP. The URL format is `<protocol>://[<username>:<password>]@<host>[:<port>][/<path>]`

File Upload

Click the **Browse** button to browse to and select a file and click the **Open** button at the File Upload dialog. The selected filename displays next to the **Browse** button.

Certificate Status

Displays the current internal web server status. Possible status is:

Switch secure HTTP certificate is presented: The certification is stored in HTTPS' database.

Switch secure HTTP certificate is not presented: No certification is stored in HTTPS' database.

Switch secure HTTP certificate is generating ...: The certification is now being generated.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Browse...: Click to display the **Choose a File to Upload** dialog box. Select a file and click **Open**.

Load: Click to load the selected certificate file.

Certificate upload via Web Browser (No File Selected):

| HTTPS Configuration | |
|----------------------|---|
| Mode | Disabled |
| Automatic Redirect | Disabled |
| Certificate Maintain | Upload |
| PassPhrase | |
| Certificate Upload | Web Browser |
| File Upload | Browse... No file selected. |
| Certificate Status | Switch secure HTTP certificate is presented |

Certificate upload via Web Browser (File Selected):

| HTTPS Configuration | |
|----------------------|---|
| Mode | Disabled |
| Automatic Redirect | Disabled |
| Certificate Maintain | Upload |
| PassPhrase | |
| Certificate Upload | Web Browser |
| File Upload | Browse... id_rsa.pub |
| Certificate Status | Switch secure HTTP certificate is presented |

Certificate upload via URL (valid path format shown in URL field):

| HTTPS Configuration | |
|----------------------|---|
| Mode | Disabled |
| Automatic Redirect | Disabled |
| Certificate Maintain | Upload |
| PassPhrase | |
| Certificate Upload | URL |
| URL | <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>] |
| Certificate Status | Switch secure HTTP certificate is presented |

Switch secure HTTP certificate is generating ...:

| HTTPS Configuration | |
|----------------------|--|
| Mode | Disabled |
| Automatic Redirect | Disabled |
| Certificate Maintain | None |
| Certificate Status | Switch secure HTTP certificate is generating ... |

Messages

Message:

*conf_sec_open failed , creating defaults
version mismatch, creating defaults
version mismatch (upgrade). Retaining the existing certificate.
HTTPS invalid certificate
HTTPS invalid URL parameter*

Meaning: An invalid HTTPS configuration was detected.

Recovery: 1. Clear the error message. 2. Re-configure the HTTPS / certificate using the procedures above.

Message: 'Certificate Maintain' can't be executed if HTTPS is enabled

Meaning: An invalid HTTPS configuration was detected.

Recovery: 1. Click the **OK** button to clear the error message. 2. Re-configure the HTTPS.

Message:

Current HTTPS mode is enabled, this operation can not be processed.

Dynamic memory allocated failure.

Invalid URL.

Upload process failure.

Invalid certificate format.

HTTPS_ERROR_CERT_TOO_BIG - The certificate PEM file size too big.

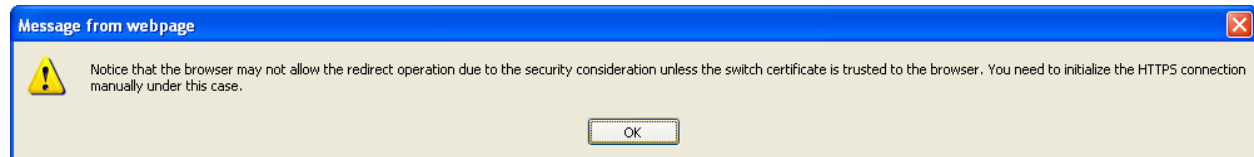
HTTPS_CERT_PRESENT - Certification is presented. No action required.

HTTPS_CERT_NOT_PRESENT - Certification is not presented.

HTTPS_CERT_IS_GENERATING - Certification is being generated. Wait for completion.

HTTPS_CERT_ERROR - Internal Error. Retry the operation.

Message: Notice that the browser may not allow the redirect operation due to the security consideration unless the switch certificate is trusted to the browser. You need to initialize the HTTPS connection manually under this case.



Meaning: Content was blocked because it was not signed by a valid security certificate. For more information, see "Certificate Errors" in Internet Explorer Help.

Recovery: 1. Click the **OK** button to clear the error message. 2. Re-configure the HTTPS.

Access Management Configuration

Configure access management table on this page from **Configuration > Security > Switch > Access Management**. You can add up to 16 entries. If the application's type matches any one of the access management entries, it will allow access to the S4224.

Click the **Add New Entry** button to start configuring a new Access Management entry. **Note:** Save each new entry individually.

| Delete | VLAN ID | Start IP Address | End IP Address | HTTP/HTTPS | SNMP | TELNET/SSH |
|--------|---------|------------------|----------------|--------------------------|--------------------------|--------------------------|
| Delete | 1 | 0.0.0.0 | 0.0.0.0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Access Management Configuration parameters:

Mode

Indicates / sets the access management mode operation. The possible modes are:

Enabled: Enable access management mode operation.

Disabled: Disable access management mode operation.

Delete

Click to delete the entry. It will be deleted during the next save.

VLAN ID

Indicates the VLAN ID for the access management entry.

Start IP Address

Indicates / sets the beginning IP address for the access management entry. The value of Start IP Address must be a valid IP address in dotted decimal notation ('x.y.z.w'). These restrictions apply:

- 1) x, y, z, and w must be decimal numbers from 0 - 255,
- 2) x must not be 0,
- 3) x must not be 127, and
- 4) x must not be greater than 223.

End IP Address

Indicates / sets the ending IP address for the access management entry. The value of End IP Address must be a valid IP address in dotted decimal notation ('x.y.z.w'). The following restrictions apply:

- 1) x, y, z, and w must be decimal numbers from 0 - 255,
- 2) x must not be 0,
- 3) x must not be 127, and
- 4) x must not be greater than 223.

HTTP/HTTPS

Check to allow the host access to the S4224 from the HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

SNMP

When checked, indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

TELNET/SSH

Check to allow the host access to the S4224 from the Telnet/SSH interface if the host IP address matches the IP address range provided in the Start IP Address / End IP Address entry (above).

Buttons

Add New Entry: Click to add a new access management entry. **Note:** Save each new entry individually.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Messages

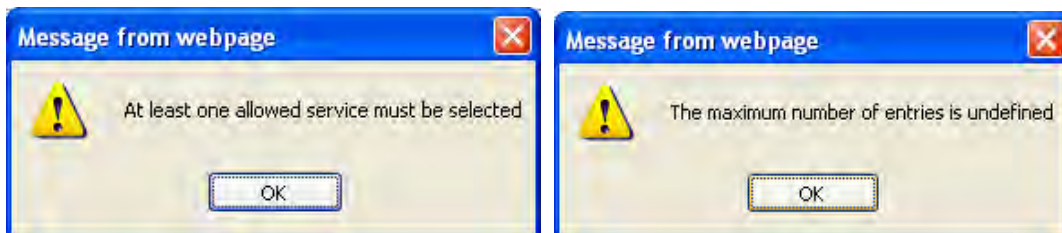
Message: *No such field: new_vid_1,2*



Meaning: On the Access Management Configuration web page, it appears that adding multiple entries before saving is possible. The **Add New Entry** button can be used and data entered multiple times, but when the **Save** button is clicked, the error pop-up displays.

Recovery: It is not possible to recover from this error; removing the multiple entry(s) and saving results in the same error (see above). You must click **OK** to clear the message, and then leave and re-access the web page before entries can again be made.

Message: *At least one allowed service must be selected*



Message: *The maximum number of entries is undefined*

Message: *There isn't any entry provide WEB service. Do you want to proceed anyway?*

SNMP Configuration

Configure SNMP on this page from the **Configuration > Security > Switch > SNMP > System** menu path.

Here you can configure S4224 SNMP System, Communities, Users, Groups, Views, Access and trap parameters. Simple Network Management Protocol (SNMP) is part of the TCP/IP protocol for network management. SNMP allows diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices running SNMP.

The SNMP agent embedded in the S4224 is capable of version 1, 2c, or v3 support to access all management information from the device. The community strings for v1 and v2c and the USM/VACM for SNMPv3 are supported. The SNMP agent can support IPv4 and IPv6 trap destinations. It also supports the INFORM PDU for notification along with traps.

Traps are generated when a condition has been met on the SNMP agent. These conditions are defined in the Management Information Base (MIB). The administrator then defines thresholds, or limits to the conditions, that are to generate a trap. Conditions range from preset thresholds to a restart.

All of the values that SNMP reports are dynamic. The information needed to get the specified values that SNMP reports is stored in the MIB. This information includes Object IDs (OIDs), Protocol Data Units (PDUs), etc. The MIBs must be located at both the agent and the manager to work effectively.

SNMP v1, v2c, v3 Descriptions

Each SNMP version is described below.

SNMPv1

SNMP version 1 (SNMPv1) is the initial implementation of the SNMP protocol. SNMPv1 operates over protocols such as User Datagram Protocol (UDP), Internet Protocol (IP), OSI Connectionless Network Service (CLNS), AppleTalk Datagram-Delivery Protocol (DDP), and Novell Internet Packet Exchange (IPX). SNMPv1 is widely used and is the de facto network-management protocol in the Internet community. The first RFCs for SNMP, now known as SNMPv1, appeared in 1988: RFC 1065, RFC 1066, and RFC 1067. These protocols were obsoleted by SNMPv1: RFC 1155, RFC 1156 and RFC 1157. After a short time, RFC 1156 (MIB-1) was replaced by the more often used *RFC 1213 - Version 2 of management information base (MIB-2) for network management of TCP/IP-based internets*. SNMPv1 was criticized for its poor security. Authentication of clients is performed only by a "community string", in effect a type of password, which is transmitted in cleartext.

SNMPv2 and v2c

SNMPv2 (RFC 1441–RFC 1452) revises SNMPv1 and includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications. It introduced GetBulkRequest, an alternative to iterative GetNextRequests for retrieving large amounts of management data in a single request. However, the new party-based security system in SNMPv2, viewed by many as overly complex, was not widely accepted.

Community-Based Simple Network Management Protocol version 2, or SNMPv2c, is defined in RFC 1901–RFC 1908. In its initial stages, this was also informally known as SNMPv1.5. SNMPv2c comprises SNMPv2 without the controversial new SNMP v2 security model, using instead the simple community-based security scheme of SNMPv1. While officially only a "Draft Standard", this is widely considered the de facto SNMPv2 standard.

User-Based Simple Network Management Protocol version 2, or SNMPv2u, is defined in RFC 1909–RFC 1910. This is a compromise that attempts to offer greater security than SNMPv1, but without incurring the high complexity of SNMPv2. A variant of this was commercialized as SNMP v2*, and the mechanism was eventually adopted as one of two security frameworks in SNMP v3.

SNMPv3

Simple Network Management Protocol Version 3 (SNMPv3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. Although SNMPv3 makes no changes to the protocol aside from the addition of cryptographic security, its developers have managed to make things look much different by introducing new textual conventions, concepts, and terminology.

SNMPv3 primarily added security and remote configuration enhancements to SNMP. Security has been the biggest weakness of SNMP since the beginning. Authentication in SNMP Versions 1 and 2 amounts to nothing more than a password (community string) sent in clear text between a manager and agent. Each SNMPv3 message contains security parameters which are encoded as an octet string. The meaning of these security parameters depends on the security model being used.

SNMPv3 provides important security features:

Confidentiality - Encryption of packets to prevent snooping by an unauthorized source.

Integrity - Message integrity to ensure that a packet has not been tampered with in transit including an optional packet replay protection mechanism.

Authentication - used to verify that the message is from a valid source.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combined security model / security level determines which security mechanism is used when handling an SNMP packet. Three security models are available: SNMPv1, v2c, and v3.

SNMPv3 introduces the following key features:

- SNMPv3 EngineID
- SNMPv3 USM (User-Based Security Model)
- SNMP VACM (View-based Access Control Model)
- SNMP Trap/Inform (v1/v2c/v3 trap, v2c/v3 inform)

The SNMPv3 function supports these services:

- SNMP v3 user management, authentication and encryption
- SNMP VACM management
- SNMP v1/v2c/v3 selection
- SNMP notification (v1/v2c/v3 trap, v2c/v3 inform) functionality

SNMP v3 EngineID concept: an SNMP engine provides services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects. There is a one-to-one association between an SNMP engine and the SNMP entity which contains it. The SNMP v3 engine contains a Dispatcher, a Message Processing Subsystem, a Security Subsystem, and an Access Control Subsystem.

Within an administrative domain, an snmpEngineID is the unique and unambiguous identifier of an SNMP engine. Since there is a one-to-one association between SNMP engines and SNMP entities, it also uniquely and unambiguously identifies the SNMP entity within that administrative domain. Note that it is possible for SNMP entities in different administrative domains to have the same value for snmpEngineID. Federation of administrative domains may necessitate assignment of new values.

SNMPv3 USM: the SNMP v3 implementation uses the traditional concept of a user (identified by a userName) with associated security information. This is a key SNMPv3 security feature implemented per RFC 3414.

SNMP v3USM User: Management operations using this Security Model make use of a defined set of user identities. For any user on whose behalf management operations are authorized at a particular SNMP engine, that SNMP engine must have knowledge of that user. An SNMP engine that wishes to

communicate with another SNMP engine must also have knowledge of a user known to that engine, including knowledge of the applicable attributes of that user.

SNMPv3 VACM: The View-based Access Control Model defines a set of services that an application (such as a Command Responder or a Notification Originator application) can use for checking access rights. Access Control occurs (either implicitly or explicitly) in an SNMP entity when processing SNMP retrieval or modification request messages from an SNMP entity. Access Control also occurs in an SNMP entity when an SNMP notification message is generated (by a Notification Originator application).

VACM includes these elements: Groups, Security Levels, Contexts, MIB Views and View Families, and Access Policy.

SNMPv3 VACM – Groups: a Group is a set of zero or more <securityModel, securityName> tuples on whose behalf SNMP management objects can be accessed. A Group defines the access rights afforded to all securityNames which belong to that group. The combination of a securityModel and a securityName maps to at most one Group. A Group is identified by a groupName.

The Access Control module assumes that the securityName has already been authenticated as needed and provides no further authentication of its own. The View-based Access Control Model uses the securityModel and the securityName as inputs to the Access Control module when called to check for access rights. It determines the groupName as a function of securityModel and securityName.

Note that when the security model is v1 or v2c, the groups "public" and "private" can not be removed, but when the security model is v3 the groups "public" and "private" can be removed.

SNMPv3 VACM – Views: Views are used to restrict the access rights of some groups to only a subset of the management information in the management domain.

A view subtree is the set of all MIB object instances which have a common ASN.1 OBJECT IDENTIFIER prefix to their names.

A family of view subtrees is a pairing of an OBJECT IDENTIFIER value (called the family name) with a bit string value (called the family mask). The family mask indicates which sub-identifiers of the associated family name are significant to the family's definition.

SNMPv3 Traps and Informs: A Trap is an SNMP message sent from one application to another (which is typically on a remote host). Their purpose is merely to notify the other application that something has happened, has been noticed, etc. The big problem with Traps is that they're unacknowledged, so you don't actually know if the remote application received your -important message. The trap is available for SNMP v1, v2c and v3.

An Inform is an acknowledged Trap. When the remote application receives an inform it sends back an acknowledgement message. Inform is available for SNMP v2c and v3. For SNMP v3, an inform must be sent to a specific remote USM user resided in the inform receiver.

SNMP v3 Users, Groups, and Views Configuration

SNMP v3 configuration involves setting up SNMP v3 Users, Groups, and Views, with the caveats discussed below. With SNMPv3, you can define SNMP users, groups, and views to provide access control to SNMP devices, and restrict certain users so they can only access the parts of the MIB that they have been given access rights to. The SNMP views, groups and users are described below.

Note: the concept of SNMP communities that was introduced in SNMPv2 is not relevant to SNMPv3, and has been replaced by SNMP groups/users. However, you can configure an S4224 to respond to both SNMPv2 and SNMPv3 commands. If both SNMPv2 and SNMPv3 are to be used, you must configure SNMP communities and SNMP groups and users. To use SNMPv1/v2c, all you need to do is add a Community; no thing else needs to be configured. You can add or delete any Communities including the default communities.

Summary: You can create multiple Views. You can then create multiple Groups, and associate them with a View. You can configure multiple Groups (each with a different Group name and security level) and associate them with a particular View. You can also configure more than one View associated with a Group (e.g., a Group with read access to the entire MIB tree, but with only write access to certain objects). You could then create multiple Users, and associate them with a Group (you can associate multiple Users with a particular Group).

With SNMPv3 you can define SNMP views, groups and users to provide access control to SNMP devices, as shown below.

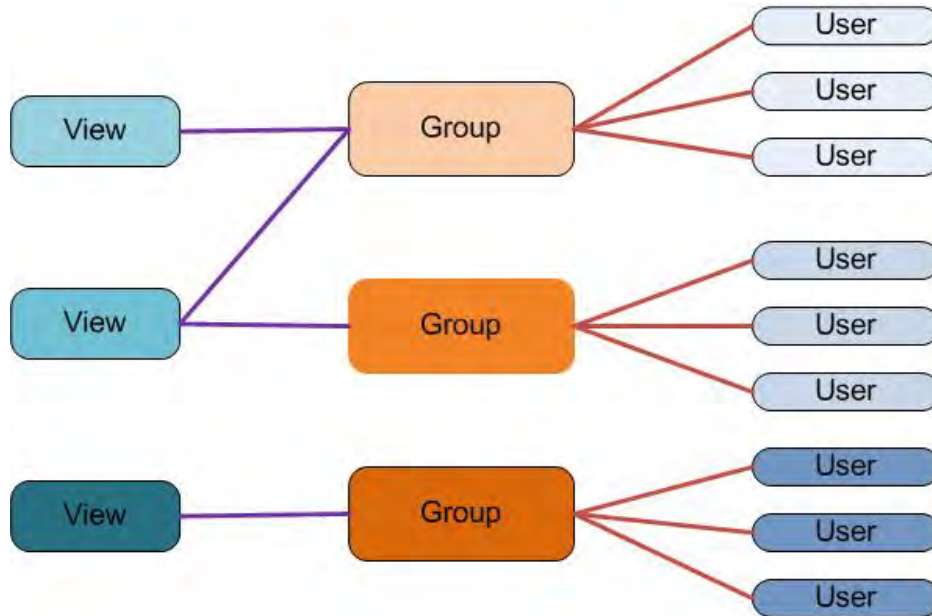


Figure 1. SNMP v3 Users, Groups, and Views

You can create multiple Views. You can then create multiple Groups, and associate them with a View. You can configure multiple Groups (each with a different Group name and security level) and associate them with a particular View. You can also configure more than one View associated with a Group (e.g., a Group with read access to the entire MIB tree, but with only write access to certain objects). You could then create multiple Users, and associate them with a Group (you can associate multiple Users with a particular Group).

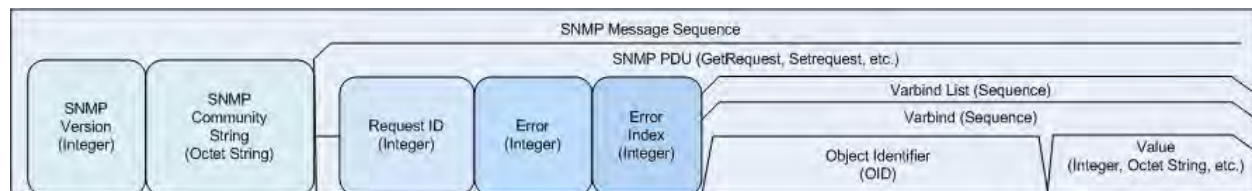
SNMP v1 Traps

Most SNMPv1 messages follow a model where a client (Network Management System) makes a request and a server (agent) responds to that request. Traps are the exception. An SNMP agent will transmit a trap to the NMS when it has a condition to report that is deemed too important to wait until asked. A common example of this is the failure of a communications link.

With most traps, the agent will include something called "'Interesting' variable bindings," which are the OID(s) and value(s) of MIB variable(s) that provide more information about the condition. So, for example, when a communications channel fails, the agent will send a pSError trap, which will have the OID of the "Link" or "Signal Detect" variable for that channel, and the value "down." Newer versions of Management Module firmware will also include bindings for the BIA (Cabinet serial number), slot, and (if applicable) subdevice of the entity in question. This information is always embedded in the first binding (as above), but are repeated separately for more convenient viewing under certain NMS packages.

SNMP v2 Traps

All S4224 SNMP Trap messages conform to SNMPv2 MIB RFC-2573. See the "Supported MIBs" section on page **Error! Bookmark not defined.** for information on support for public (standard) and private MIBs. A sample SNMP Message sequence is shown below.



SNMP v3 Traps

The SNMP v3 traps are mainly SNMPv2 traps with added authentication and privacy capabilities. SNMPv3 Traps use the engineID of the local application sending the trap rather than the engineID of the remote application. This means that you must create users in your remote user database and create one for each engineID you wish to send traps from.

See "[Appendix E: SNMP Traps and MIBs](#)" on page 615 for the list of SNMP traps.

SNMP v3 Configuration Process

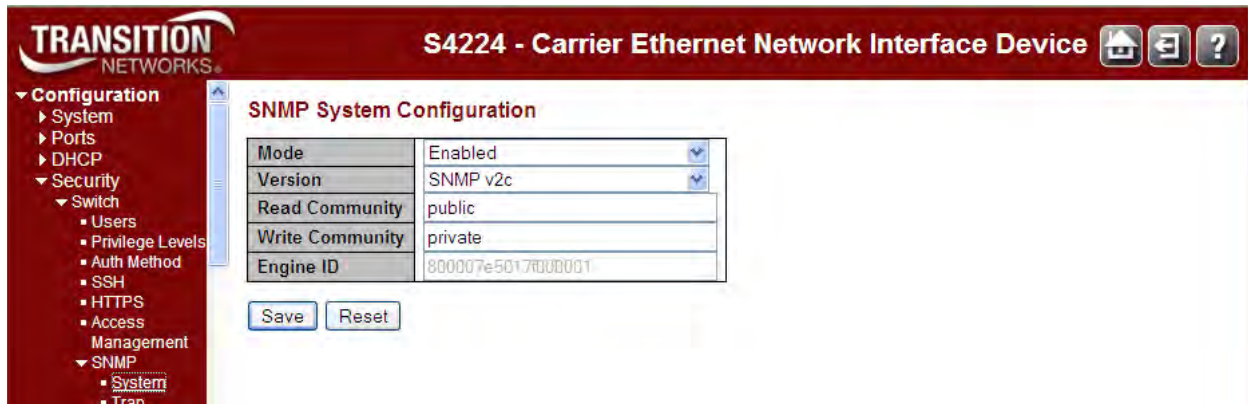
Perform these procedures to configure the S4224 for SNMP v3.

- System** - see [SNMP System Configuration](#) on page 71.
- Trap** - see [SNMP Trap Configuration](#) on page 72.
- Communities** - see [SNMPv3 Community Configuration](#) on page 77.
- Users** - see [SNMPv3 User Configuration](#) on page 78.
- Groups** - see [SNMPv3 Group Configuration](#) on page 80.
- Views** - see [SNMPv3 View Configuration](#) on page 81.
- Access** - see [SNMPv3 Access Configuration](#) on page 82.

The procedures in this process are defined in the following sections.

SNMP System Configuration

The default **Configuration > Security > Switch > SNMP > System** page is shown below. Note that the SNMP parameters displayed will vary depending on the SNMP Trap version selected.



The **Configuration > Security > Switch > SNMP > System** parameters are explained below.

Mode

Sets the SNMP mode operation. Possible modes are:

Enabled: Enable SNMP mode operation (default).

Disabled: Disable SNMP mode operation.

Version

Sets the SNMP supported version. Possible versions are:

SNMP v1: Set SNMP support to version 1.

SNMP v2c: Set SNMP support to version 2c (default).

SNMP v3: Set SNMP support to version 3.

Read Community

Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The default is **'public'**.

The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet. This field is grayed out if 'SNMP v3' is selected.

Write Community

Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 - 255, and the allowed content is the ASCII characters from 33 to 126. The default is **'private'**.

The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet. This field is grayed out if 'SNMP v3' is selected.

Engine ID

Indicates the SNMPv3 engine ID. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-F's are not allowed (e.g., 800007e5017f000001). Changing the Engine ID clears (deletes) all original local users. This field is grayed out unless 'SNMP V3' is selected.

SNMP Trap Configuration

Configure SNMP traps on this page from the **Configuration > Security > Switch > SNMP > Trap** menu path. This page provides SNMP configuration features with support for Multiple Trap destinations on SNMPv1 Traps, SNMPv2c Inform and SNMPv3 Traps. The default Trap Configuration page is shown below.

Trap Configuration

Global Settings

Mode: Disabled

Trap Destination Configurations

| Delete | Name | Enable | Version | Destination Address | Destination Port |
|---------------|------|--------|---------|---------------------|------------------|
| Add New Entry | | | | | |
| Save Reset | | | | | |

Click the **Add New Entry** button to display the default SNMP Trap Configuration / Trap Event page:

SNMP Trap Configuration

| | |
|-------------------------------|----------|
| Trap Config Name | |
| Trap Mode | Disabled |
| Trap Version | SNMP v2c |
| Trap Community | Public |
| Trap Destination Address | |
| Trap Destination Port | 162 |
| Trap Inform Mode | Disabled |
| Trap Inform Timeout (seconds) | 3 |
| Trap Inform Retry Times | 5 |
| Trap Probe Security Engine ID | Enabled |
| Trap Security Engine ID | |
| Trap Security Name | None |

SNMP Trap Event

| | | |
|----------------|---|-------------------------------------|
| System | <input type="checkbox"/> * <input type="checkbox"/> Warm Start | <input type="checkbox"/> Cold Start |
| Interface | Link up <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches | |
| | * Link down <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches | |
| | LLDP <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches | |
| Authentication | <input type="checkbox"/> * <input type="checkbox"/> SNMP Authentication Fail | |
| Switch | <input type="checkbox"/> * <input type="checkbox"/> STP | <input type="checkbox"/> RMON |

Save Reset

Trap Config Name

Indicates which trap Configuration's name for configuring. The allowed string length is **1** to **32**, and the allowed content is ASCII characters from **33** to **126**.

Trap Mode

Sets the SNMP trap mode operation. The valid selections are:

Enabled: Enable SNMP trap mode operation.

Disabled: Disable SNMP trap mode operation (default).

Trap Version

Sets the SNMP trap supported version. The valid selections are:

SNMP v1: Set SNMP trap support to SNMP version 1.

SNMP v2c: Set SNMP trap support to SNMP version 2c (default).

SNMP v3: Set SNMP trap support to SNMP version 3.

Trap Community

Sets the community access string when sending an SNMP trap packet. The allowed string length is **0** to **255**, and the allowed content is ASCII characters from **33** to **126**. The default is '**public**'.

Trap Destination Address

Sets the SNMP trap destination address. Enter a valid IP address in dotted decimal notation (x.y.z.w), with these restrictions:

- 1) x, y, z, and w must be decimal numbers from **0-255**,
- 2) x must not be 0 unless x, y, and w are also **0**,
- 3) x must not be **127**, and
- 4) x must not be greater than **223**.

Indicates the SNMP trap destination IPv4 address. It allows a valid IPv4 address in dotted decimal notation ('x.y.z.w') or a valid hostname. A valid hostname is a string drawn from the alphabet (A-Z, a-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Trap Destination Port

Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is **1-65535**. The default is port **162**.

Trap Inform Mode

Sets the SNMP trap inform mode operation. Not configurable in SNMP v1 mode. Valid selections are:

Enabled: Enable SNMP trap inform mode operation.

Disabled: Disable SNMP trap inform mode operation.

Trap Inform Timeout (seconds)

Sets the SNMP trap inform timeout. Not configurable in SNMP v1 mode. The valid range is **0** - **2147**. The default is **1**.

Trap Inform Retry Times

Sets the SNMP trap inform retry times. Not configurable in SNMP v1 mode. The valid range is 0 - 255. The default is 5.

Trap Probe Security Engine ID

Sets the SNMP V3 trap probe security engine ID mode of operation. The valid values are:

Enabled: Enable SNMP trap probe security engine ID mode of operation (default).

Disabled: Disable SNMP trap probe security engine ID mode of operation.

This field displays only if the 'Trap Version' parameter is set to **SNMP v3** (see the 'Trap Version' description above).

Trap Security Engine ID

Sets the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number (in hexadecimal format) with between 10 and 64 characters, but all-zeros and all-'F's are not allowed. The message "Probe Fail" displays if the information could not be read.

This field displays only if the 'Trap Version' parameter is set to **SNMP v3** (see the 'Trap Version' description above).

Trap Security Name

Sets the SNMP trap security name. SNMPv3 traps and informs use USM for authentication and privacy. A unique security name is needed when traps and informs are enabled. The default is **None**.

This field displays only if the 'Trap Version' parameter is set to **SNMP v3** (see the 'Trap Version' description above).

SNMP Trap Event

Configure SNMP trap in this section.

SNMP Trap Event

| | | |
|-----------------------|--|-------------------------------------|
| System | <input type="checkbox"/> * <input type="checkbox"/> Warm Start | <input type="checkbox"/> Cold Start |
| Interface | Link up <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches | |
| | *Link down <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches | |
| | LLDP <input checked="" type="radio"/> none <input type="radio"/> specific <input type="radio"/> all switches | |
| Authentication | <input type="checkbox"/> * <input type="checkbox"/> SNMP Authentication Fail | |
| Switch | <input type="checkbox"/> * <input type="checkbox"/> STP | <input type="checkbox"/> RMON |

System

Enable/disable the Interface group's traps. Possible traps are:

Warm start: Enable/disable Warm Start trap.

Cold start: Enable/disable Cold Start trap.

Interface

Sets the Interface group's traps. Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible traps are:

Link Up: Enable/disable Link up trap for none / specific / all switches).

Link Down: Enable/disable Link down trap for none / specific / all switches).

LLDP: Enable/disable LLDP trap for none / specific / all switches).

Authentication

Indicates that the AAA group's traps. Possible traps are:

SNMP Authentication Fail : Enable/disable SNMP trap authentication failure trap.

Switch

Indicates that the Switch group's traps. Possible traps are:

STP: Enable/disable STP trap.

RMON: Enable/disable RMON trap.

Specific Trap Event Configuration

If you select the 'specific' radio button for the SNMP Trap Events 'Link up', 'Link down', and 'LLDP', the port-specific table displays. Configure the events on a per-port basis as required. Click the **Save** button when done.

| Port | Link up | Link down | LLDP |
|------|-------------------------------------|-------------------------------------|-------------------------------------|
| * | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 4 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 5 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 6 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Example

A Trap Config example is shown below.

Trap Configuration

Global Settings

Mode: Enabled

Trap Destination Configurations

| Delete | Name | Enable | Version | Destination Address | Destination Port |
|--------------------------|-----------------------|---------|---------|---------------------|------------------|
| <input type="checkbox"/> | Trap1 | Enabled | SNMPv2c | 192.168.1.30 | 162 |
| <input type="checkbox"/> | Trap2 | Enabled | SNMPv1 | 192.168.1.30 | 162 |
| <input type="checkbox"/> | Trap3 | Enabled | SNMPv3 | 192.168.1.30 | 162 |

Add New Entry

Save Reset

You can click the **Name** link (e.g., [Trap1](#) above) to display its instance config page.

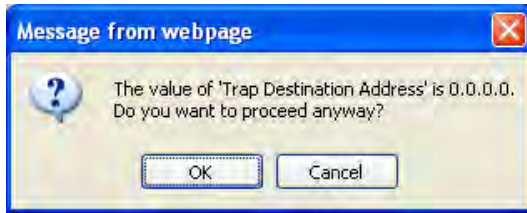
Buttons

Save: Click to save changes.

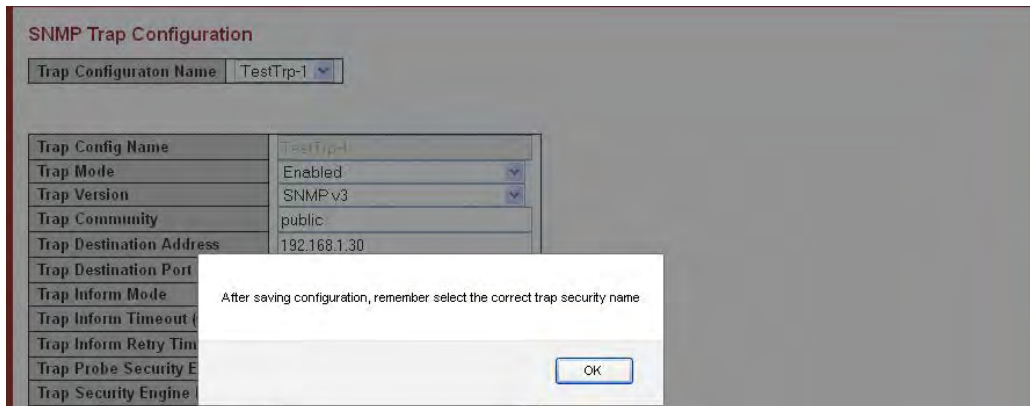
Reset: Click to undo any changes made locally and revert to previously saved values.

Messages

Message: The value of "Trap Destination Address" is 0.0.0.0. Do you want to proceed anyway?



Message: After saving configuration, remember select the correct trap security name

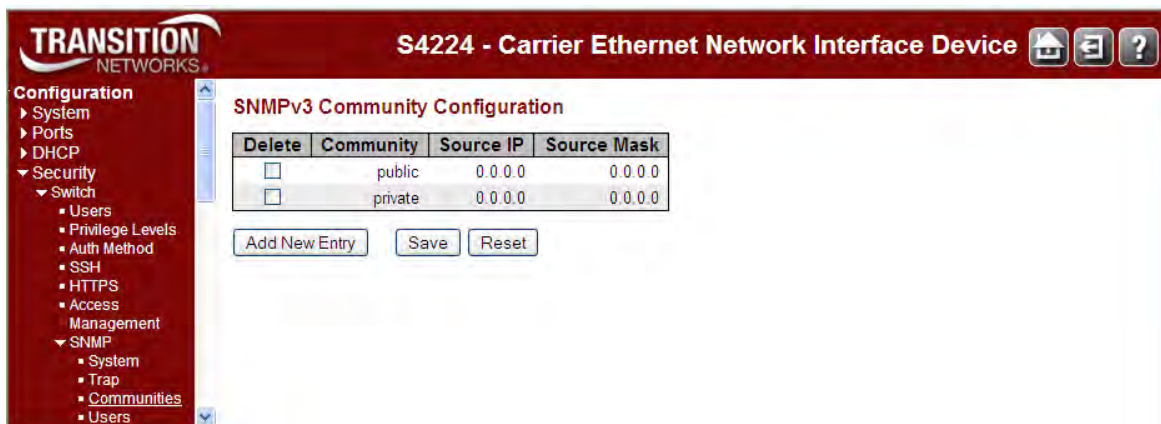


Recovery: 1. Click the **OK** button to clear the message. 2. Enter the parameter as described above.

SNMPv3 Community Configuration

Configure SNMPv3 community table on this page from the **Configuration > Security > Switch > SNMP > Communities** menu path. The entry index key is **Community**. SNMP V1 and V2c use a community string match for authentication. SNMP V3 uses a username match for authentication, or authentication based on the HMAC-MD5 or HMAC-SHA algorithms.

From the default page, click the **Add New Entry** button to display the new entry edit fields.



Delete

Check to delete the entry. It will be deleted during the next save.

Community

Indicates / sets the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32 characters, and the allowed content is ASCII characters from 33 to 126 (e.g., space character not allowed). The community string will be treated as the security name and map an SNMPv1 or SNMPv2c community string.

Source IP

Indicates / sets the SNMP access source address. A particular range of source addresses can be used to restrict the source subnet when combined with source mask (e.g., **192.168.1.30**).

Source Mask

Indicates / sets the SNMP access source address mask (e.g., **255.255.255.0**). Enter a valid IP mask of a dotted decimal string ('x.y.z.w'), where:

- 1) x, y, z, and w are decimal numbers from **0-255**, and
- 2) when converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero.

Buttons

Add New Entry: Click to add a new SNMP community entry. Enter the Community, Source IP, and Source Mask as described above.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

SNMPv3 User Configuration

Configure SNMPv3 user table on this page from the **Configuration - Security - Switch - SNMP > User** menu path. The entry index keys are **Engine ID** and **User Name**.

The USM is supported per standard with a variety of user access levels and privacy protocols.

SNMP v3 configuration involves setting up SNMP v3 Users, Groups, and Views. SNMP Users have a specified username, authentication password, privacy password, (if required) and authentication and privacy protocol assigned. The authentication protocol options are none, MD5, or SHA. The privacy algorithm options are none, AES, or DES. When a new User is created, it is associated with an SNMP group.

From the default page, click the **Add New Entry** button to display the new entry edit fields.

| Delete | Engine ID | User Name | Security Level | Authentication Protocol | Authentication Password | Privacy Protocol | Privacy Password |
|--------------------------|----------------------|----------------------|----------------|-------------------------|-------------------------|------------------|----------------------|
| <input type="checkbox"/> | 800007e5017f000001 | default_user | NoAuth, NoPriv | None | None | None | None |
| Delete | <input type="text"/> | <input type="text"/> | Auth, Priv | MD5 | <input type="text"/> | DES | <input type="text"/> |

Delete

Check to delete the entry. It will be deleted during the next save.

Engine ID

An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equals system engine ID then it is local user; otherwise it's remote user.

User Name

A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters 33 to 126. No spaces can be entered.

Security Level

Indicates the security model that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.

Note: if **Security Level** is set to **NoAuth, NoPriv**, then the remaining fields do not require an entry or selection.

Authentication Protocol

Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

None: No authentication protocol.

MD5: An optional flag to indicate that this user uses MD5 authentication protocol.

SHA: An optional flag to indicate that this user uses SHA authentication protocol.

The value of security level cannot be modified if entry already exists. That means that you must first ensure that the value is set correctly.

Authentication Password

A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40 characters. The allowed content is ASCII characters from 33 to 126.

Privacy Protocol

Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

None: No privacy protocol.

DES: An optional flag to indicate that this user uses DES authentication protocol.

Privacy Password

A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126. No space characters are allowed.

Buttons

Add New Entry: Click to add a new user entry. Enter the Engine ID, User Name, Security Level, and Auth / Privacy entries as described above.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

SNMPv3 Group Configuration

Configure SNMPv3 group table on this page from the **Configuration > Security > Switch > SNMP > Group** menu path. The entry index keys are Security Model and Security Name.

SNMP v3 configuration involves setting up SNMP v3 Users, Groups, and Views. SNMP Groups are basically access control policies to which users can be added. Each SNMP Group is configured with a security model, and is associated with an SNMP security name. These parameters specify the type of authentication and privacy a user within the SNMP group will use, and also which objects in the MIB the User can access. Each SNMP Group name and security level pair must be unique within the device.

From the default page, click the **Add New Entry** button to display the new entry edit fields.

| Delete | Security Model | Security Name | Group Name |
|--------------------------|----------------|---------------|------------------|
| <input type="checkbox"/> | v1 | public | default_ro_group |
| <input type="checkbox"/> | v1 | private | default_rw_group |
| <input type="checkbox"/> | v2c | public | default_ro_group |
| <input type="checkbox"/> | v2c | private | default_rw_group |
| <input type="checkbox"/> | usm | default_user | default_rw_group |

Delete

Check to delete the entry. It will be deleted during the next save.

Security Model

Indicates / sets the security model that this entry should belong to. Possible security models are:

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

Security Name

A string identifying the security name that this entry should belong to. The allowed string length is **1** to **32**, and the allowed content is ASCII characters from 33 to 126 (e.g., no space characters).

Group Name

A string identifying the group name that this entry should belong to. The allowed string length is **1** to **32**, and the allowed content is ASCII characters from 33 to 126 (e.g., no space characters).

Buttons

Add New Entry: Click to add a new group entry to the table. Enter the Security Model, Security Name, and associated Group Name as discussed above.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

SNMPv3 Views Configuration

Configure SNMPv3 view table on this page from the **Configuration > Security > Switch > SNMP > Group** menu path. The entry index keys are View Name and OID Subtree.

SNMP v3 configuration involves setting up SNMP v3 Users, Groups, and Views. SNMP MIB Views are defined lists of objects within a MIB that can be used to control which parts of a MIB can be accessed by Users belonging to the SNMP Group associated with that particular View. Objects in the View may be from anywhere in the MIB, and are not required to be in the same MIB sub-tree. When you have defined your Views, you must configure for your SNMP Groups the type of access Users will have to those Views.

From the default page, click the **Add New Entry** button to display the new entry edit fields.

| Delete | View Name | View Type | OID Subtree |
|---------------------------------------|----------------------|-----------|----------------------|
| <input type="checkbox"/> | default_view | included | .1 |
| <input type="button" value="Delete"/> | <input type="text"/> | included | <input type="text"/> |

Delete

Check the checkbox to delete the entry. It will be deleted during the next save.

View Name

A string identifying the view name that this entry should belong to. The allowed string length is **1 - 32**, and the allowed content is ASCII characters from **33 - 126**.

View Type

Indicates the view type that this entry should belong to. Possible view types are:

included: An optional flag to indicate that this view subtree should be included.

excluded: An optional flag to indicate that this view subtree should be excluded.

In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and its OID subtree should overstep the 'excluded' view entry.

OID Subtree

The OID defining the root of the subtree to add to the named view. The format of the OID Subtree is .OID1.OID2.OID3... The allowed OID length is **.1** to **.128**. The valid string content is a digital number or asterisk (*).

Buttons

Add New view: Click to add a new View entry to the table. Enter the View Name, View Type, and OID Subtree as described above.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

SNMPv3 Access Configuration

Configure the SNMPv3 access table on this page from the **Configuration > Security > Switch > SNMP > Access** menu path. The entry index keys are **Group Name**, **Security Model** and **Security Level**. The default table displays two Groups: **default_ro_group** and **default_rw_group**. You can edit the **Read View Name** and the **Write View Name** for each of the two default entries in the initial table.

When you click the **Add New Entry** button, the SNMPv3 access table displays with fields for the new access group.

| Delete | Group Name | Security Model | Security Level | Read View Name | Write View Name |
|--------------------------|------------------|----------------|----------------|----------------|-----------------|
| <input type="checkbox"/> | default_ro_group | any | NoAuth, NoPriv | default_view | None |
| <input type="checkbox"/> | default_rw_group | any | NoAuth, NoPriv | default_view | default_view |

Buttons: Add New Entry, Save, Reset

Delete

Check to delete the entry. It will be deleted during the next Save.

Group Name

A string identifying the group name that this entry belongs to. Valid string lengths are **1** to **32**, and the allowed content is ASCII characters from 33 to 126. This dropdown lets you select an existing Group Name.

Security Model

Indicates the security model that this entry should belong to. Valid security models are:

any: Any SNMP security model accepted (v1, v2c, or usm).

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

Security Level

Indicates the security model that this entry should belong to. Valid security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication but no privacy.

Auth, Priv: Authentication and privacy.

Read View Name

The name of the MIB view defining the MIB objects for which this request may request the current values.

The allowed string length is **1** to **32**, and the allowed content is ASCII characters from **33** to **126**.

The dropdown lets you select an existing Read View Name or **None**.

Write View Name

The name of the MIB view defining the MIB objects for which this request may potentially set new values.

The allowed string length is **1** to **32**, and the allowed content is ASCII characters from 33 to 126.

The dropdown lets you select an existing Write View Name or **None**.

Buttons

Add New Entry: Click to add a new access entry to the table. Add the Group Name, Security Model, Security Level, Read View Name, and Write View Name as described above.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Configuration > Security > Switch > RMON

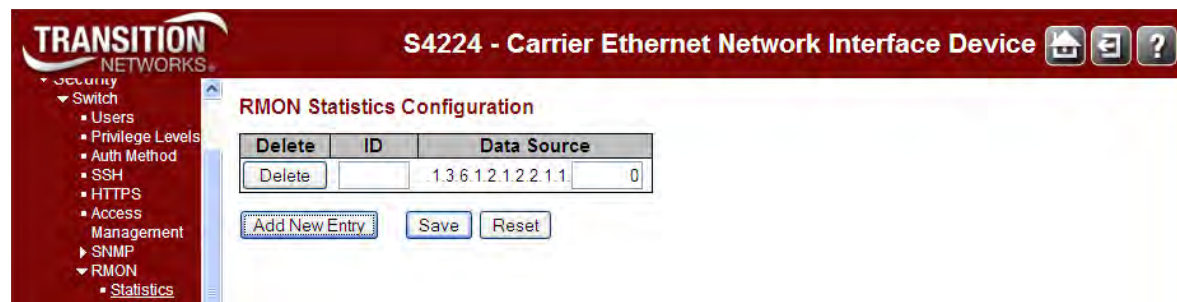
Configure RMON Statistics, History, Alarms, and Events from the **Configuration > Security > Switch > RMON** menu path. The S4224 RMON (Remote Network Monitoring) function supports the monitoring and protocol analysis of a LAN per [IETF RFC 1271](#). A part of SNMP, RMON is a network management protocol that gathers remote network information.

RMON collects nine kinds of information, including packets sent, bytes sent, packets dropped, statistics by host, by conversations between two sets of addresses, and certain kinds of events that have occurred. A network administrator can find out how much bandwidth or traffic each user is imposing on the network and what Web sites are being accessed. Alarms can be set to alert you of impending problems. The RMON Statistics, History, Alarm, and event data displays at **Monitor > Security > Switch > RMON > Event**.

RMON > Statistics

The **Configuration > Security > Switch > RMON > Statistics** menu path displays the **RMON Statistics Configuration** page. Configure RMON Statistics table on this page. The entry index key is **ID**. The initial table displays no entries.

When you click the **Add New Entry** button, the RMON access table displays with fields for the new access group. You can edit the ID and the Data Source port suffix field in the table.



The RMON Statistics table parameters are explained below.

Delete

Click to delete the entry. It will be deleted during the next save.

ID

Enter the index for this entry. The valid range is **1** to **65535**.

Data Source

Indicates the port ID which you want to be monitored (e.g., **1.3.6.1.2.1.2.2.1.1.0**). The valid range is **1-1013**.

Buttons

Add New Entry: Click to add a new community entry to the table. Add the ID and Data Source entries as described above.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

RMON > History

The **Configuration > Security > Switch > RMON > History** menu path displays the RMON History Configuration table. Configure RMON History table on this page. The entry index key is **ID**.

From the default screen, click the **Add New Entry** button to display the new entry fields.

| Delete | ID | Data Source | Interval | Buckets | Buckets Granted |
|--------|----|----------------------|----------|---------|-----------------|
| Delete | | .1.3.6.1.2.1.2.2.1.1 | 0 | 1800 | 50 |

Buttons: Add New Entry, Save, Reset

The RMON History table parameters are explained below.

Delete

Check to delete the entry. It will be deleted during the next save.

ID

Indicates the index of the entry. The valid range is **1** to **65535**.

Data Source

Indicates the port ID which you want to be monitored with RMON.

Interval

Indicates the interval in seconds for sampling the history statistics data. The valid range is **1** to **3600**. The default value is **1800** seconds.

Buckets

Indicates the maximum data entries associated this History control entry stored in RMON. The valid range is **1** to **3600**. The default value is **50**. This is the RMON "buckets requested" value - the requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this historyControlEntry. When this object is created or modified, the probe should set historyControlBucketsGranted as closely to this object as is possible for the particular probe implementation and available resources. The default is **50**.

Buckets Granted

The number of data saved in the RMON. The number of discrete sampling intervals over which data will be saved in the part of the media-specific table associated with this *historyControlEntry*.

See the RMON RFC ([IETF RFC 2819](#)) for details on the particular probe implementation and available resources.

Buttons

Add New Entry: Click to add a new community entry to the table. Enter the ID, Data Source, Interval, Buckets, and Buckets Granted parameters.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

The example below shows two valid, saved RMON statistics table entries.

The screenshot displays the 'RMON History Configuration' web interface. It features a table with the following columns: Delete, ID, Data Source, Interval, Buckets, and Buckets Granted. Below the table are three buttons: 'Add New Entry', 'Save', and 'Reset'.

| Delete | ID | Data Source | Interval | Buckets | Buckets Granted |
|--------------------------|----|---------------------|----------|---------|-----------------|
| <input type="checkbox"/> | 1 | 1.3.6.1.2.1.2.2.1.1 | 1 | 900 | 50 |
| <input type="checkbox"/> | 2 | 1.3.6.1.2.1.2.2.1.1 | 2 | 50 | 50 |

Buttons: Add New Entry, Save, Reset

RMON > Alarm

The **Configuration > Security > Switch > SNMP > RMON > Alarm** menu path displays the RMON Alarm Configuration table. Configure RMON Alarm table on this page. The entry index key is **ID**.

When you click the **Add New Entry** button from the default table page, the table displays with entry fields.

| Delete | ID | Interval | Variable | Sample Type | Value | Startup Alarm | Rising Threshold | Rising Index | Falling Threshold | Falling Index |
|--------|----|----------|------------------------|-------------|-------|-----------------|------------------|--------------|-------------------|---------------|
| Delete | | 30 | .1.3.6.1.2.1.2.2.1.0.0 | Delta | 0 | RisingOrFalling | 0 | 0 | 0 | 0 |

The RMON Alarm Configuration table parameters are explained below.

Delete

Click to delete the entry on this line. If not previously saved, it will be deleted immediately; otherwise, it will be deleted during the next save.

ID

Indicates / set the port index of the entry. The valid range is **1** to **65535**.

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The valid range is **1** to **2³¹-1**.

Variable

Enter a variable value in the format *xxx.yyy*, where *xxx* is 10-21, and *yyy* is 1-65,535.

Indicates the particular variable to be sampled. The valid variables are:

InOctets: The total number of octets received on the interface, including framing characters.

InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol.

InNUcastPkts: The number of broadcast and multi-cast packets delivered to a higher-layer protocol.

InDiscards: The number of inbound packets that are discarded even the packets are normal.

InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

InUnknownProtos: the number of the inbound packets that were discarded because of the unknown or un-support protocol.

OutOctets: The number of octets transmitted out of the interface, including framing characters.

OutUcastPkts: The number of unicast packets that request to transmit.

OutNUcastPkts: The number of broadcast and multi-cast packets that request to transmit.

OutDiscards: The number of outbound packets that are discarded in the event the packet is normal.

OutErrors: The number of outbound packets that could not be transmitted because of errors.

OutQLen: The length of the output packet queue (in packets).

Sample Type

The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

- Absolute:** Get the sample directly.
- Delta:** Calculate the difference between samples (default).

Value

The value of the statistic during the last sampling period.

Startup Alarm

The method of sampling the selected variable and calculating the value to be compared against the thresholds. The valid sample types are:

- Rising:** Trigger alarm when the first value is larger than the rising threshold.
- Falling:** Trigger alarm when the first value is less than the falling threshold.
- RisingOrFalling:** Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).

Rising Threshold

Rising threshold value (-2147483648 - 2147483647). The Rising Threshold must be larger than the Falling Threshold.

Rising Index

Rising event index (1 - 65535). The Rising Threshold must be larger than the Falling Threshold.

Falling Threshold

Falling threshold value (-2147483648 - 2147483647). The Falling Threshold must be smaller than the Rising Threshold.

Falling Index

Falling event index (1 - 65535). The Falling Index must be smaller than the Rising Index.

Buttons

Add New Entry: Click to add a new community entry.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

A table with two new RMON Alarm Configuration entries is shown below.

| Delete | ID | Interval | Variable | Sample Type | Value | Startup Alarm | Rising Threshold | Rising Index | Falling Threshold | Falling Index |
|--------------------------|----|----------|-------------------------|-------------|------------|-----------------|------------------|--------------|-------------------|---------------|
| <input type="checkbox"/> | 1 | 30 | 1.3.6.1.2.1.2.2.1.10.1 | Delta | 1 | RisingOrFalling | 2 | 2 | 1 | 1 |
| <input type="checkbox"/> | 6 | 30 | 1.3.6.1.2.1.2.2.1.20.10 | Absolute | 2148435712 | Rising | 20 | 10 | 10 | 9 |

RMON > Event

The **Configuration > Security > Switch > SNMP > RMON > Event** menu path displays the RMON Alarm Configuration table. Configure RMON Event table on this page. The entry index key is **ID**.

When you click the **Add New Entry** button from the default table page, the table displays with entry fields.

| Delete | ID | Desc | Type | Community | Event Last Time |
|--------|----------------------|----------------------|------|-----------|-----------------|
| Delete | <input type="text"/> | <input type="text"/> | none | public | 0 |

The RMON Event table parameters are explained below.

Delete

Click to delete the entry. If not previously saved, it will be deleted immediately; otherwise it will be deleted during the next save.

ID

Enter the index of the RMON event. The valid range is **1** to **65535**. Each ID entry must be unique.

Desc

Indicates this event, the string length is **0** to **127**. The default is a **null** string.

Type

Indicates the notification of the event, the valid types are:

none: No logging action is performed.

log: A syslog entry is added.

snmptrap: A SNMP trap event is sent.

logandtrap: A syslog entry is logged and an SNMP trap event is sent.

Community

Specify the community when a trap is sent; the string length is **0** to **127** characters. The default is **"public"**.

Event Last Time

Indicates the value of sysUpTime at the time this event entry last generated an event (e.g., 33554560 or 33 days, 55 hours, 45 minutes, and 50 seconds).

Buttons

Add New Entry: Click to add a new community entry to the table. Enter the ID, Desc, Type, Community, and Event Last Time values as described above.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

An RMON Event Configuration table with four entries is shown below (IDs 1-4).

| Delete | ID | Desc | Type | Community | Event Last Time |
|--------------------------|----|-------------|------------|-----------|-----------------|
| <input type="checkbox"/> | 1 | rmon event1 | logandtrap | public | 1935766625 |
| <input type="checkbox"/> | 2 | rmonevt_2 | snmptrap | public | 1935766625 |
| <input type="checkbox"/> | 3 | rmonevt3 | log | public | 1818391920 |
| <input type="checkbox"/> | 4 | rmonevt4 | none | public | 1818391920 |

Buttons: Add New Entry, Save, Reset

Note that you can monitor the related RMON Statistics, History, Alarm, and Event data from the **Monitor > Security > Switch > RMON > Event** menu path.

Related RMON RFCs

RFC 2819 - [RMON1](#) - Remote Network Monitoring Management Information Base

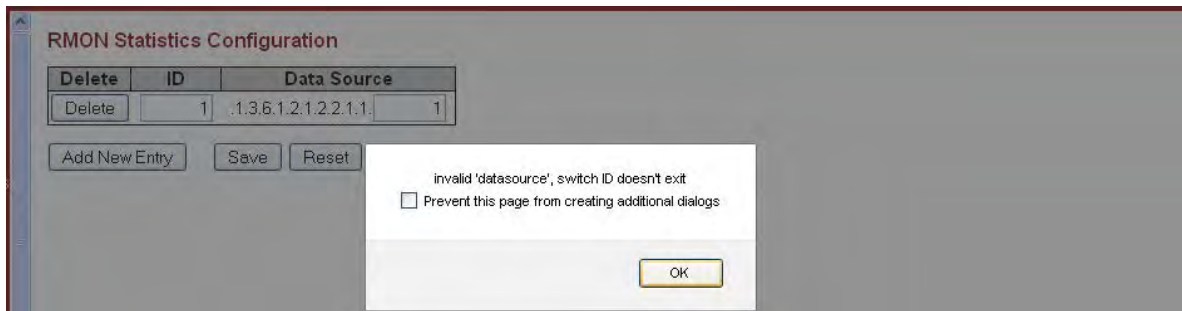
RFC 4502 - [RMON2](#) - Remote Network Monitoring Management Information Base Version 2 using SMIv2

RFC 2613 - [SMON](#) - Remote Network Monitoring MIB Extensions for Switched Networks

RFC 3577 - [Overview](#) - Introduction to the RMON Family of MIB Modules

Messages

Message: invalid 'datasource', switch ID doesn't exist
Prevent this page from creating additional dialogs



Port Security Limit Control Configuration

Configuration > Security > Network > Limit Control

The **Configuration > Security > Network > Limit Control** menu path lets you to configure the Port Security Limit Control system-level and port-level settings.

Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions described below.

The Limit Control module utilizes a lower-layer module (the Port Security module) which manages MAC addresses learned on the port. The Limit Control configuration consists of two sections, a system-wide and a port-wide configuration table.

The screenshot shows the web interface for an S4224 Carrier Ethernet Network Interface Device. The left sidebar contains a navigation tree with 'Configuration' > 'Security' > 'Network' > 'Limit Control' selected. The main content area is titled 'Port Security Limit Control Configuration' and includes a 'Refresh' button. The 'System Configuration' section has the following settings:

| | |
|---------------|--------------------------|
| Mode | Disabled |
| Aging Enabled | <input type="checkbox"/> |
| Aging Period | 3600 seconds |

The 'Port Configuration' section displays a table with the following data:

| Port | Mode | Limit | Action | State | Re-open |
|------|----------|-------|--------|----------|---------|
| * | <> | 4 | <> | | |
| 1 | Disabled | 4 | None | Disabled | Reopen |
| 2 | Disabled | 4 | None | Disabled | Reopen |
| 3 | Disabled | 4 | None | Disabled | Reopen |
| 4 | Disabled | 4 | None | Disabled | Reopen |
| 5 | Disabled | 4 | None | Disabled | Reopen |
| 6 | Disabled | 4 | None | Disabled | Reopen |
| 7 | Disabled | 4 | None | Disabled | Reopen |
| 8 | Disabled | 4 | None | Disabled | Reopen |
| 9 | Disabled | 4 | None | Disabled | Reopen |

System Configuration

Mode

Indicates if Limit Control is globally enabled or disabled on the S4224. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

Aging Enabled

If checked, secured MAC addresses are subject to aging as discussed under 'Aging Period' below. To keep the MAC table updated, an aging scan is conducted to remove entries that were not recently accessed. This ensures that stations moved to new locations are not permanently prevented from receiving frames in their new location. It also frees up MAC table entries occupied by obsolete stations to make room for new stations. The IEEE 802.1d recommends 300 seconds per entry.

Aging Period

If checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

The Aging Period can be set to a number between **10** and **10,000,000** seconds. The IEEE 802.1d recommends **300** seconds per entry.

To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Port Configuration

At Port Security Limit Control Configuration, the Port Configuration table has one row for each S4224 port a number of columns, which are explained below.

Port

The port number to which the configuration below applies. The * in the Port column acts as a 'wild card' character which causes the selections in this row to be applied to all other rows in the table for which this selection is valid.

Mode

Controls whether Limit Control is enabled on this port. Both this and the 'Global Mode' must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.

Limit

The maximum number of MAC addresses that can be secured on this port. Enter a number from **1** - **1024**. If this limit is exceeded, the corresponding action is taken. The S4224 is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

Action

If the 'Limit' defined above is reached, the S4224 can take one of the following actions:

None: Do not allow more than 'Limit' MAC addresses on the port, but take no further action.

Trap: If 'Limit' + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.

Shutdown: If 'Limit' + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down.

There are three ways to re-open the shutdown port:

- 1) Boot the S4224.
- 2) Disable and re-enable Limit Control on the port or the S4224, or
- 3) Click the **Reopen** button.

Trap & Shutdown: If 'Limit' + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

State

This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:

Disabled: Limit Control is either globally disabled or disabled on the port.

Ready: The limit is not yet reached. This can be shown for all actions.

Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if 'Action' is set to **None** or **Trap**.

Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if 'Action' is set to **Shutdown** or to **Trap & Shutdown**.

Re-open Button

If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to the **Shutdown** description in the Action section above.

Note: clicking the **Reopen** button causes the page to be refreshed, so non-committed (unsaved) changes will be lost.

Buttons

Refresh: Click to refresh the page. Note that non-committed (unsaved) changes will be lost.

Reset: Click to undo any changes made locally and revert to previously saved values.

Save: Click to save changes.

NAS (Network Access Server) Configuration

Configuration > Security > Network > NAS

The **Configuration > Security > Network > NAS** menu path lets you configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network.

These backend (RADIUS) servers are configured from the **Configuration > Security > AAA** menu path.

The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as explained below.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his system. A device uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

IEEE 802.1X Port-based Network Access Control provides a standard for authenticating and authorizing devices attached to a LAN port. Generally, IEEE 802.1X is port-based; however, the S4224 also supports MAC-based network access control.

The NAS configuration consists of two sections, for system-wide and port-wide NAS configuration.

Network Access Server Configuration Refresh

System Configuration

| | |
|--------------------------------|--------------------------|
| Mode | Disabled |
| Reauthentication Enabled | <input type="checkbox"/> |
| Reauthentication Period | 3600 seconds |
| EAPOL Timeout | 30 seconds |
| Aging Period | 300 seconds |
| Hold Time | 10 seconds |
| RADIUS-Assigned QoS Enabled | <input type="checkbox"/> |
| RADIUS-Assigned VLAN Enabled | <input type="checkbox"/> |
| Guest VLAN Enabled | <input type="checkbox"/> |
| Guest VLAN ID | 1 |
| Max. Reauth. Count | 2 |
| Allow Guest VLAN if EAPOL Seen | <input type="checkbox"/> |

Port Configuration

| Port | Admin State | RADIUS-Assigned QoS Enabled | RADIUS-Assigned VLAN Enabled | Guest VLAN Enabled | Port State | Restart |
|------|------------------|-----------------------------|------------------------------|--------------------------|-------------------|-----------------------------|
| * | <> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| 1 | Force Authorized | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate Reinitialize |
| 2 | Force Authorized | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate Reinitialize |
| 3 | Force Authorized | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate Reinitialize |
| 4 | Force Authorized | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate Reinitialize |
| 5 | Force Authorized | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate Reinitialize |
| 6 | Force Authorized | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate Reinitialize |
| 7 | Force Authorized | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate Reinitialize |
| 8 | Force Authorized | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate Reinitialize |
| 9 | Force Authorized | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate Reinitialize |
| 10 | Force Authorized | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate Reinitialize |
| 11 | Force Authorized | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Globally Disabled | Reauthenticate Reinitialize |

The NAS page parameters are explained below.

NAS System Configuration

Mode

Indicates if NAS is globally enabled or disabled on the S4224. If globally disabled, all ports are allowed forwarding of frames.

Reauthentication Enabled

If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).

Reauthentication Period

Sets the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range **1** to **3600** seconds.

EAPOL Timeout

Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range **1** to **65535** seconds. This has no effect on MAC-based ports.

Aging Period

This setting applies to the following modes (i.e., modes using the Port Security function) to secure MAC addresses:

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between **10** and **1000000** seconds.

If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.

For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

Hold Time

This setting applies to the following modes (i.e., modes using the Port Security functionality to secure MAC addresses):

- Single 802.1X
- Multi 802.1X
- MAC-Based Auth.

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "**Configuration > Security > AAA**" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication.

In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.

The Hold Time can be set to a number between **10** and **1000000** seconds.

RADIUS-Assigned QoS Enabled

RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description).

The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

RADIUS-Assigned VLAN Enabled

RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see 'RADIUS-Assigned VLAN Enabled' below for a detailed description).

The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

Guest VLAN Enabled

A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

Guest VLAN ID

This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are **1** - **255**.

Max. Reauth. Count

The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are **1** - **255**.

Allow Guest VLAN if EAPOL Seen

The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port.

The value can only be changed if the Guest VLAN option is globally enabled.

NAS Port Configuration

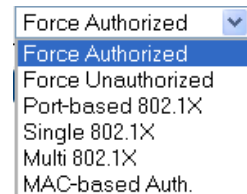
The table has one row for each S4224 port and a number of columns, which are explained below.

Port

The port number for which the configuration below applies. The * in the Port column acts as a 'wild card' character which causes the selections in this row to be applied to all other rows in the table for which this selection is valid.

Admin State

If NAS is globally enabled, this selection controls the port's authentication mode. Note that the 802.1x Admin State must be set to **Force Authorize** for ports enabled for Spanning Tree. The Spanning Tree function is configured at **Configuration > Spanning Tree > CIST Ports > CIST Normal Port Configuration** in the "STP Enabled" column.



The following modes are available:

Force Authorized: In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

Force Unauthorized: In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

Port-based 802.1X: In 802.1X, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs ([RFC3748](#)). Frames sent between the switch and the RADIUS server are **RADIUS** packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like [MD5-Challenge](#), [PEAP](#), and [TLS](#). The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Single 802.1X: In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant.

Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If

more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X: Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant.

An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.

The maximum number of supplicants that can be attached to a port can be limited using the 'Port Security Limit Control' functionality.

MAC-based Auth.: Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). The switch only supports the [MD5-Challenge](#) authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users (equipment whose MAC address is a valid RADIUS user can be used by anyone). Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

RADIUS-Assigned QoS Enabled

When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes:

- Port-based 802.1X
- Single 802.1X

RADIUS attributes used in identifying a QoS Class:

The `User-Priority-Table` attribute defined in [RFC4675](#) forms the basis for identifying the QoS Class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range 0' - ', which translates into the desired QoS Class in the range 0 - 7.

RADIUS-Assigned VLAN Enabled

When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes:

- Port-based 802.1X
- Single 802.1X

For troubleshooting VLAN assignments, use the **Monitor > VLANs > VLAN Membership** and the **Monitor > VLANs > VLAN Port** menu paths. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

RADIUS attributes used in identifying a VLAN ID:

IETF [RFC2868](#) and [RFC3580](#) form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

- The `Tunnel-Medium-Type`, `Tunnel-Type`, and `Tunnel-Private-Group-ID` attributes must all be present at least once in the Access-Accept packet.
- The switch looks for the first set of these attributes that have the same `Tag` value and fulfill the following requirements (if `Tag == 0` is used, the `Tunnel-Private-Group-ID` does not need to include a `Tag`):
 - Value of `Tunnel-Medium-Type` must be set to "IEEE-802" (ordinal 6).
 - Value of `Tunnel-Type` must be set to "VLAN" (ordinal 13).
 - Value of `Tunnel-Private-Group-ID` must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1- 4094].

Guest VLAN Enabled

When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.

This option is only available for EAPOL-based modes, i.e.:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

For trouble-shooting VLAN assignments, use the **Monitor > VLANs > VLAN Membership** and the **Monitor > VLANs > VLAN Port** pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

Guest VLAN Operation:

When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds the 'Max. Reauth. Count' and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest

VLAN. The interval between transmissions of EAPOL Request Identity frames is configured with 'EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen' enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's 'Admin State' is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

Port State

The current state of the port. It can undertake one of the following values:

Globally Disabled: NAS is globally disabled.

Link Down: NAS is globally enabled, but there is no link on the port.

Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.

Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.

X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently, **X** clients are authorized and **Y** are unauthorized.

Restart

Two buttons in the 'Restart' column are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.

Clicking these buttons will not cause settings changed on the page to take effect.

Reauthenticate: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.

This button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

Reinitialize: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.



Buttons

Refresh: Click to refresh the page.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Example

In the sample **Configuration > Security > NAS** setup below, Port 3 shows “Single 802.1X”, RADIUS-assigned QoS disabled / VLAN disabled, Guest VLAN enabled, Authorized port state, with “Reauthenticate” and “Reinitialize” restart enabled.

Network Access Server Configuration
Refresh

System Configuration

| | |
|--------------------------------|-------------------------------------|
| Mode | Enabled |
| Reauthentication Enabled | <input type="checkbox"/> |
| Reauthentication Period | 3600 seconds |
| EAPOL Timeout | 30 seconds |
| Aging Period | 300 seconds |
| Hold Time | 10 seconds |
| RADIUS-Assigned QoS Enabled | <input checked="" type="checkbox"/> |
| RADIUS-Assigned VLAN Enabled | <input checked="" type="checkbox"/> |
| Guest VLAN Enabled | <input checked="" type="checkbox"/> |
| Guest VLAN ID | 1 |
| Max. Reauth. Count | 2 |
| Allow Guest VLAN if EAPOL Seen | <input checked="" type="checkbox"/> |

Port Configuration

| Port | Admin State | RADIUS-Assigned QoS Enabled | RADIUS-Assigned VLAN Enabled | Guest VLAN Enabled | Port State | Restart |
|------|-------------------|-------------------------------------|-------------------------------------|-------------------------------------|-----------------|-----------------------------|
| * | <> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | |
| 1 | Force Authorized | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Authorized | Reauthenticate Reinitialize |
| 2 | Port-based 802.1X | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Link Down | Reauthenticate Reinitialize |
| 3 | Single 802.1X | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Link Down | Reauthenticate Reinitialize |
| 4 | Multi 802.1X | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Link Down | Reauthenticate Reinitialize |
| 5 | MAC-based Auth. | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 0 Auth/0 Unauth | Reauthenticate Reinitialize |
| 6 | Force Authorized | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Link Down | Reauthenticate Reinitialize |

The 802.1X Admin State must be set to ‘Authorized’ for ports that are enabled for Spanning Tree. You can disable STP at the port level at **Configuration > Spanning Tree > CIST Port** menu path by unchecking the “STP Enabled” checkbox.

Note that the two buttons in the ‘Restart’ column are available for the Port 3 row. The **Reauthenticate** and **Reinitialize** buttons are only enabled when authentication is globally enabled and the port’s Admin State is in an EAPOL-based or MAC-based mode.

ACL Ports Configuration

Configure the ACL parameters (ACE) of each S4224 port from the **Configuration > Security > Network > ACL > Ports** menu path. The ACL Ports Configuration parameters will affect frames received on a port unless the frame matches a specific ACE.

Access Controls Lists

The S4224 can 'peek' into the frames at line rate and is capable of deep packet inspection; this ability gives a wide range of access controls. The rules or the access control lists can look at any field in the Layer 2 to Layer 4 headers to make the decision of allowing, discarding, mirroring, logging or even shutdown the port that the frame came through.

The ACL rule created can be associated with any port as well when created as a policy.

Apart from the ACL, there is a device level option to do storm prevention for the unicast, multicast and broadcast frames.

ACE (Access Control Entry) describes access permissions associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

S4224 - Carrier Ethernet Network Interface Device

ACL Ports Configuration

| Port | Policy ID | Action | Rate Limiter ID | Port Redirect | Logging | Shutdown | State | Counter |
|------|-----------|--------|-----------------|---------------|----------|----------|---------|---------|
| * | 0 | <> | <> | <> | <> | <> | <> | * |
| 1 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 2 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 3 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 4 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 5 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 6 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 7 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 8 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 9 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 10 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 11 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 12 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 13 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 14 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 15 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 16 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 17 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 18 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 19 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 20 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 21 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 22 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 23 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 24 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 25 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 26 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 27 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |
| 28 | 0 | Permit | Disabled | Disabled | Disabled | Disabled | Enabled | 0 |

Buttons: Refresh, Clear, Save, Reset

The **Configuration > Security > Network > ACL > Ports** page parameters are explained below.

Port

The logical port for the settings contained in the same row. The * in the Port column acts as a 'wild card' character which causes the selections in this row to be applied to all other rows in the table for which this selection is valid.

Policy ID

Select the policy to apply to this port. The allowed values are 0 - 8. The default value is 0.

Action

Select whether forwarding is permitted (**Permit**) or denied (**Deny**). The default value is **Permit**. Note that Action can not be set to Permit with a 'Port Copy' setting of other than Disabled.

Rate Limiter ID

Select which rate limiter to apply on this port. The allowed values are **Disabled** or the values 1 - 16. The default value is **Disabled**. **Note:** The ACL rate limiter and EVC policer can not both be enabled.

EVC Policer

Select whether EVC policer is enabled or disabled. The default value is **Disabled**. **Caution:** the ACL policer and the EVC policer can not both be enabled at the same time.

EVC Policer ID

Select which EVC policer ID to apply on this port. The valid values are **Disabled** or 1 -128.

Port Redirect

Select which port frames are copied on. The allowed values are **Disabled** or a specific port number. The default value is **Disabled**. Note that 'Action' can not be set to Permit with a Port Redirect setting of other than **Disabled**.

Mirror

Specify the mirror operation of this port. The allowed values are:
Enabled: Frames received on the port are mirrored.
Disabled: Frames received on the port are not mirrored.
The default value is " **Disabled** ".

Logging

Specify the logging operation of this port. The allowed values are:
Enabled: Frames received on the port are stored in the System Log.
Disabled: Frames received on the port are not logged.
The default value is " **Disabled** ". Please note that the System Log memory size and logging rate is limited.

Shutdown

Specify the port shut down operation of this port. The allowed values are:
Enabled: If a frame is received on the port, the port will be disabled.
Disabled: Port shut down is disabled.
The default value is " **Disabled** ".

State

Specify the port state of this port. The allowed values are:
Enabled: To reopen ports by changing the volatile port configuration of the ACL user module.

Disabled: To close ports by changing the volatile port configuration of the ACL user module. The default value is " **Enabled** ".

Counter

A count of the number of frames that match this ACE. This is a read only field.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page; any changes made locally will be undone.

Clear: Click to clear the counters.

ACL Rate Limiter Configuration

Configure the rate limiter for the ACL of the S4224 from the **Configuration > Security > Network > ACL > Rate Limiters** menu path.

ACL Rate Limiter Configuration

| Rate Limiter ID | Rate (pps) |
|-----------------|------------|
| * | 1 |
| 1 | 1 |
| 2 | 1 |
| 3 | 1 |
| 4 | 1 |
| 5 | 1 |
| 6 | 1 |
| 7 | 1 |
| 8 | 1 |
| 9 | 1 |
| 10 | 1 |
| 11 | 1 |
| 12 | 1 |
| 13 | 1 |
| 14 | 1 |
| 15 | 1 |
| 16 | 1 |

Save Reset

The **Configuration > Security > Network > ACL > Rate Limiters** page parameters are explained below.

Rate Limiter ID

The rate limiter ID for the settings contained in the same row. The * in the Rate Limiter ID column acts as a 'wild card' character which causes the selections in this row to be applied to all other rows in the table for which this selection is valid.

Rate (pps)

Specify the rate unit. The valid rates are **0-131071** pps (packets per second).

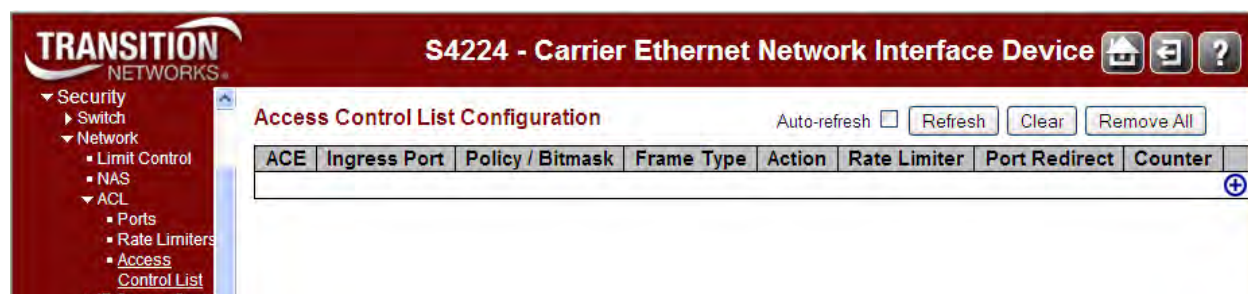
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Access Control List (ACL) Configuration

The **Configuration > Security > Network > ACL > Access Control List** menu path displays the Access Control List Configuration table, which is made up of the ACEs defined on this S4224. Each row describes the ACE that is defined. The maximum number of ACEs is **512** on each S4224.



Click on the lowest plus sign(+) to add a new ACE to the list. The reserved ACEs used for internal protocol cannot be edited or deleted, the order sequence cannot be changed, and the priority is highest.

ACE

Indicates the ACE ID.

Ingress Port

Indicates the ingress port of the ACE. Possible values are:

all: The ACE will match all ingress port.

port: The ACE will match a specific ingress port.

Policy / Bitmask

Indicates the policy number and bitmask of the ACE.

Frame Type

Indicates the frame type of the ACE. Possible values are:

any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.

IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.

IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.

IPv4/other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.

IPv6: The ACE will match all IPv6 standard frames.

Action

Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter

Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Redirect

Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are **Disabled** or a specific port number. When **Disabled** is displayed, the port redirect operation is disabled.

Mirror

Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

Counter

The counter indicates the number of times the ACE was hit by a frame.

ACE Configuration

The ACE Configuration page displays when you click on the plus sign (+) to add a new ACE to the list.

Each ACE (Access Control Entry) describes access permissions associated with a particular ACE ID. There are nine ACE frame types (Any, EType, IPv4, IPv4/ICMP, IPv4/UDP, IPv4/TCP, IPv4/Other and IPv6) and three ACE actions (Permit, Deny, and Filter). The ACE also contains many detailed, varied parameter options that are available for individual application.

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected.

A frame that hits this ACE matches the configuration that is defined here.

The screenshot shows the 'ACE Configuration' page for a device named 'S4224 - Carrier Ethernet Network Interface Device'. The left sidebar contains a navigation tree with 'Security' expanded to 'ACL' > 'Access Control List'. The main content area is divided into several sections:

- ACE Configuration:**
 - Ingress Port: All
 - Policy Filter: Any
 - Frame Type: Any
- Action:** Permit
- Rate Limiter:** Disabled
- Logging:** Disabled
- Shutdown:** Disabled
- Counter:** 0
- MAC Parameters:**
 - DMAC Filter: Any
- VLAN Parameters:**
 - VLAN ID Filter: Any
 - Tag Priority: Any

At the bottom of the configuration area are 'Save', 'Reset', and 'Cancel' buttons.

The **Configuration > Security > Network > ACL > Access Control List** page parameters are explained below.

Ingress Port

Select the ingress port for which this ACE applies.

all: The ACE applies to all port.

port n: The ACE applies to this port number, where *n* is the number of the switch port.

Policy Filter

Specify the policy number filter for this ACE.

any: No policy filter is specified (policy filter status is "don't-care").

specific: If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears.

Policy Value

When "Specific" is selected for the policy filter, you can enter a specific policy value. The valid range is 0 - 63.

Policy Bitmask

When "Specific" is selected for the policy filter, you can enter a specific policy bitmask.

The allowed range is 0x0 to 0x3f. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [policy_value & policy_bitmask].

For example, if the policy value is 3 and the policy bitmask is 0x10 (bit 0 is "don't-care" bit), then policy 2 and 3 are applied to this rule.

Frame Type

Select the frame type for this ACE. These frame types are mutually exclusive.

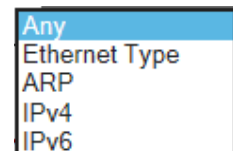
any: The ACE will match any frame type.

Ethernet Type: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. The EtherType is a field in the Ethernet MAC header, used to indicate which protocol is being transported in an Ethernet frame.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

IPv6: The ACE will match all IPv6 standard frames.



Action

Specify the action to take with a frame that hits this ACE.

Permit: The frame that hits this ACE is granted permission for the ACE operation.

Deny: The frame that hits this ACE is dropped.

Rate Limiter

Specify the rate limiter in number of base units. The allowed range is 1 to 16. **Disabled** indicates that the rate limiter operation is disabled.

Port Redirect

Frames that hit the ACE are redirected to the port number specified here. The rate limiter will affect these ports. The allowed range is the same as the switch port number range. **Disabled** indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted.

Logging

Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information. The allowed values are:

Enabled: Frames matching the ACE are stored in the System Log.

Disabled: Frames matching the ACE are not logged.

Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.

Shutdown

Specify the port shut down operation of the ACE. The allowed values are:

Enabled: If a frame matches the ACE, the ingress port will be disabled.

Disabled: Port shut down is disabled for the ACE.







Note: The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).

Counter

The counter indicates the number of times the ACE was hit by a frame.

Modification Buttons

You can modify each ACE (Access Control Entry) in the table using the following buttons:

- : Inserts a new ACE before the current row. Use this button initially (from the default screen) to create an initial ACE.
- : Edits the ACE row.
- : Moves the ACE up the list.
- : Moves the ACE down the list.
- : Deletes the ACE.
- : The lowest plus sign adds a new entry at the bottom of the ACE listings.



These Modification buttons display in the far-right column of the Access Control List Configuration table.


Buttons

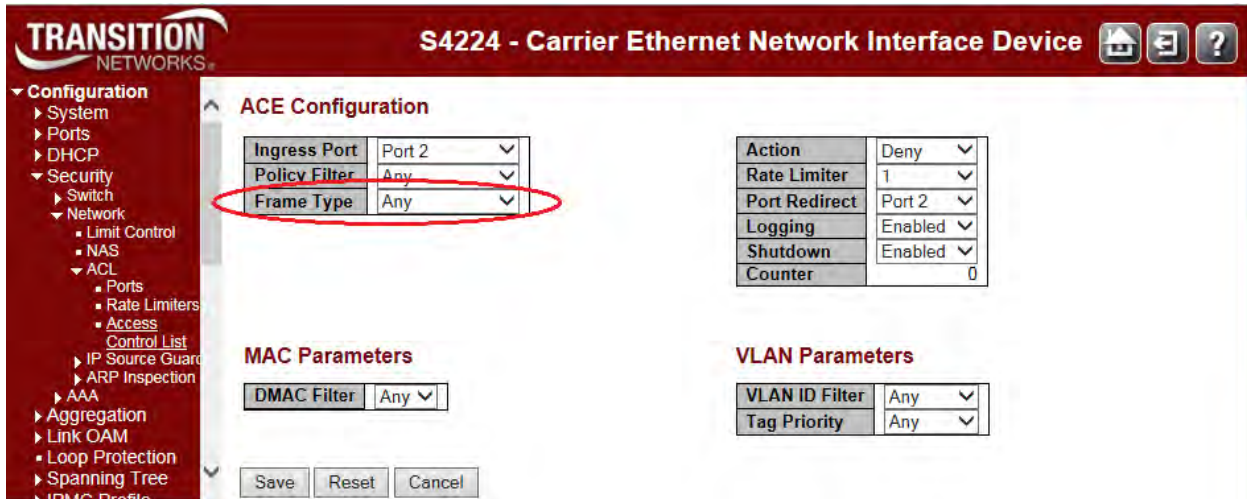
Auto-refresh: Check to refresh the page automatically. Automatic refresh occurs every three seconds.

Refresh: Click to refresh the page; any changes made locally will be undone.

Clear: Click to clear the Counter column in the table.

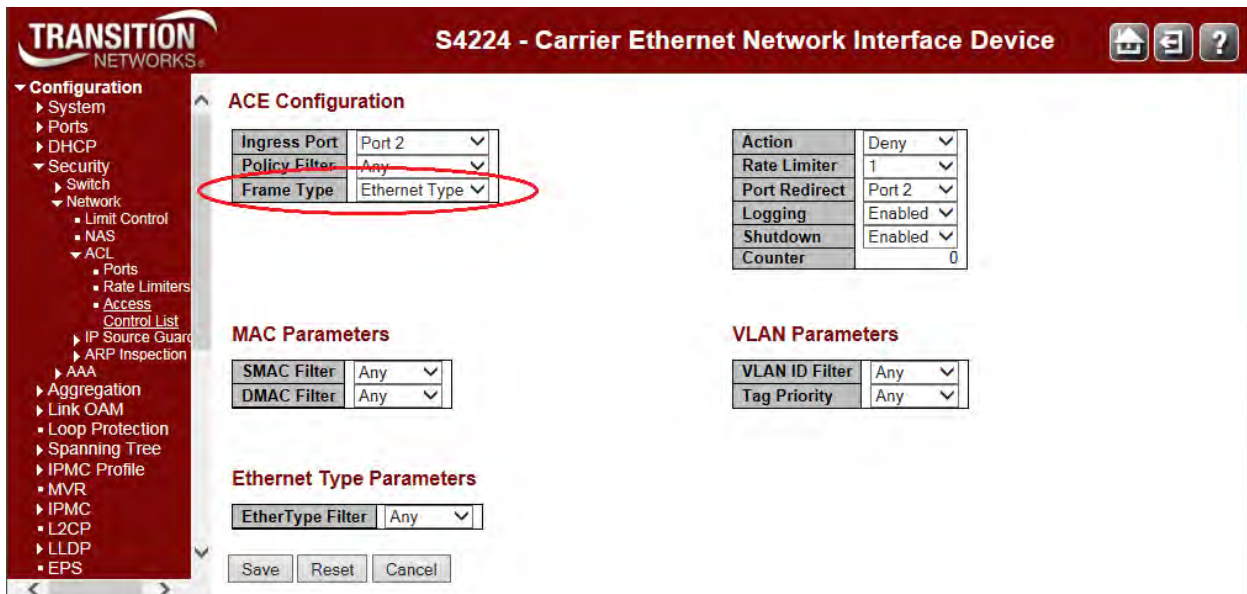
Remove All: Click to remove all existing ACE entries from the tables. At the confirm prompt, click **OK** to proceed.

When you click the  button to edit an existing ACE row, the ACE row edit screen displays to let you edit the above parameters for an existing ACE entry.



The parameters displayed depend on the config selections. For example, the config screen above displays if you select **Frame Type** = **Any**.

The configuration screen below displays if you select **Frame Type** = **Ethernet Type**.



The configuration screen below displays if you select **Frame Type = ARP**.

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

Configuration

- System
- Ports
- DHCP
- Security
 - Switch
 - Network
 - Limit Control
 - NAS
 - ACL
 - Ports
 - Rate Limiters
 - Access Control List
 - IP Source Guard
 - ARP Inspection
 - AAA
 - Aggregation
 - Link OAM
 - Loop Protection
 - Spanning Tree
 - IPMC Profile
 - MVR
 - IPMC
 - L2CP
 - LLDP
 - EPS
 - MEP
 - ERPS
 - MAC Table
 - VLAN Translation

ACE Configuration

| | |
|---------------|--------|
| Ingress Port | Port 2 |
| Policy Filter | Any |
| Frame Type | ARP |

| | |
|---------------|---------|
| Action | Deny |
| Rate Limiter | 1 |
| Port Redirect | Port 2 |
| Logging | Enabled |
| Shutdown | Enabled |
| Counter | 0 |

MAC Parameters

| | |
|-------------|-----|
| SMAC Filter | Any |
| DMAC Filter | Any |

ARP Parameters

| | |
|------------------|-----|
| ARP/RARP | Any |
| Request/Reply | Any |
| Sender IP Filter | Any |
| Target IP Filter | Any |

VLAN Parameters

| | |
|----------------|-----|
| VLAN ID Filter | Any |
| Tag Priority | Any |

ARP Sender MAC Match

| | |
|-----------------------|-----|
| ARP Sender MAC Match | Any |
| RARP Target MAC Match | Any |
| IP/Ethernet Length | Any |
| IP | Any |
| Ethernet | Any |

Save Reset Cancel

The configuration screen below displays if you select **Frame Type = IPv4**.

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

Configuration

- System
- Ports
- DHCP
- Security
 - Switch
 - Network
 - Limit Control
 - NAS
 - ACL
 - Ports
 - Rate Limiters
 - Access Control List
 - IP Source Guard
 - ARP Inspection
 - AAA
 - Aggregation
 - Link OAM
 - Loop Protection
 - Spanning Tree
 - IPMC Profile
 - MVR
 - IPMC
 - L2CP
 - LLDP
 - EPS
 - MEP
 - ERPS
 - MAC Table
 - VLAN Translation
 - VLANs

ACE Configuration

| | |
|---------------|--------|
| Ingress Port | Port 2 |
| Policy Filter | Any |
| Frame Type | IPv4 |

| | |
|---------------|---------|
| Action | Deny |
| Rate Limiter | 1 |
| Port Redirect | Port 2 |
| Logging | Enabled |
| Shutdown | Enabled |
| Counter | 0 |

MAC Parameters

| | |
|-------------|-----|
| DMAC Filter | Any |
|-------------|-----|

IP Parameters

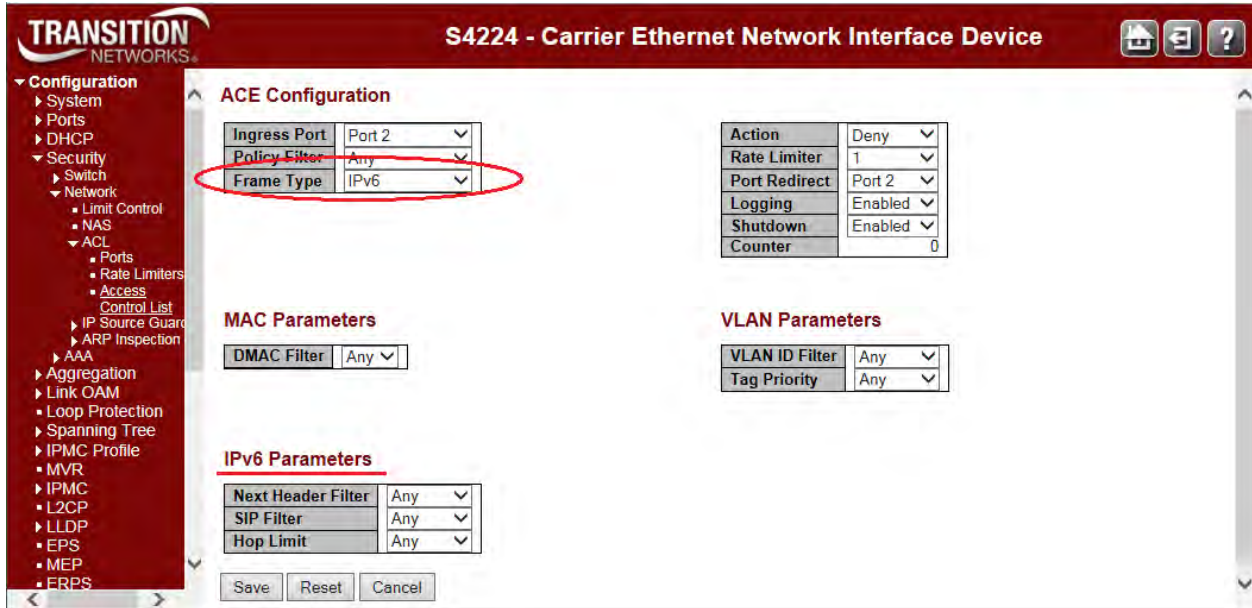
| | |
|--------------------|-----|
| IP Protocol Filter | Any |
| IP TTL | Any |
| IP Fragment | Any |
| IP Option | Any |
| SIP Filter | Any |
| DIP Filter | Any |

VLAN Parameters

| | |
|----------------|-----|
| VLAN ID Filter | Any |
| Tag Priority | Any |

Save Reset Cancel

The configuration screen below displays if you select **Frame Type = IPv6**.



The various ACL parameters are explained below.

ACE Configuration Parameters

The ACE Configuration parameters let you configure the Access Control List Configuration table parameters as described earlier in this section.

ACE Configuration

| | | |
|---------------|------|---|
| Ingress Port | All | ▼ |
| Policy Filter | Any | ▼ |
| Frame Type | IPv6 | ▼ |

| | | |
|---------------|---------|---|
| Action | Deny | ▼ |
| Rate Limiter | 1 | ▼ |
| Port Redirect | Port 2 | ▼ |
| Logging | Enabled | ▼ |
| Shutdown | Enabled | ▼ |
| Counter | 0 | |

MAC Parameters

SMAC Filter

Specify the source MAC filter for this ACE. (Only displayed when the frame type is Ethernet Type or ARP.)

Any: No SMAC filter is specified. (SMAC filter status is "don't-care".)

Specific: If you want to filter a specific source MAC address with this ACE, choose this value.

A field for entering an SMAC value displays.

MAC Parameters

| | | |
|-------------|-----|---|
| SMAC Filter | Any | ▼ |
| DMAC Filter | Any | ▼ |

SMAC Value

When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxx" (x is a hexadecimal digit).

A frame that hits this ACE matches this SMAC value.

MAC Parameters

| | | |
|-------------|-------------------|---|
| SMAC Filter | Specific | ▼ |
| SMAC Value | 00-00-00-00-00-01 | |
| DMAC Filter | Any | ▼ |

DMAC Filter

Specify the destination MAC filter for this ACE.

Any: No DMAC filter is specified. (DMAC filter status is "don't-care".)

MC: Frame must be multicast.

BC: Frame must be broadcast.

UC: Frame must be unicast.

MAC Parameters

| | | |
|-------------|-----|---|
| SMAC Filter | Any | ▼ |
| DMAC Filter | Any | ▼ |

- MC
- BC
- UC

DMAC Value

When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.

VLAN Parameters

VLAN ID Filter

Specify the VLAN ID filter for this ACE.

Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)

Specific: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number displays.

VLAN Parameters

| | |
|----------------|----------|
| VLAN ID Filter | Specific |
| VLAN ID | 1 |
| Tag Priority | 4-7 |

VLAN ID

When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The valid range is 1 to 4094. A frame that hits this ACE matches this VLAN ID value.

Tag Priority

Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The valid number range is 0 to 7. The value **Any** means that no tag priority is specified (tag priority is "don't-care".)

ARP Parameters

The ARP parameters can be configured when Frame Type "ARP" is selected.

ARP Parameters

| | |
|------------------|-----|
| ARP/RARP | Any |
| Request/Reply | Any |
| Sender IP Filter | Any |
| Target IP Filter | Any |

| | |
|-----------------------|-----|
| ARP Sender MAC Match | Any |
| RARP Target MAC Match | Any |
| IP/Ethernet Length | Any |
| IP | Any |
| Ethernet | Any |

ARP/RARP

Specify the available ARP/RARP opcode (OP) flag for this ACE.

Any: No ARP/RARP OP flag is specified. (OP is "don't-care".)

ARP: Frame must have ARP opcode set to ARP.

RARP: Frame must have RARP opcode set to RARP.

Other: Frame has unknown ARP/RARP Opcode flag.

Request/Reply

Specify the available Request/Reply opcode (OP) flag for this ACE.

Any: No Request/Reply OP flag is specified. (OP is "don't-care".)

Request: Frame must have ARP Request or RARP Request OP flag set.

Reply: Frame must have ARP Reply or RARP Reply OP flag.

Sender IP Filter

Specify the sender IP filter for this ACE.

Any: No sender IP filter is specified. (Sender IP filter is "don't-care".)

Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.

Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.

Sender IP Address

When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

Sender IP Mask

When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.

Target IP Filter

Specify the target IP filter for this specific ACE.

Any: No target IP filter is specified. (Target IP filter is "don't-care".)

Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears. **Network:** Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.

Target IP Address

When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

Target IP Mask

When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.

ARP Sender MAC Match

Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.

0: ARP frames where SHA is not equal to the SMAC address.

1: ARP frames where SHA is equal to the SMAC address.

Any: Any value is allowed ("don't-care").

RARP Target MAC Match

Specify whether frames can hit the action according to their target hardware address (THA) field settings.

0: RARP frames where THA is not equal to the target MAC address.

1: RARP frames where THA is equal to the target MAC address.

Any: Any value is allowed ("don't-care").

IP/Ethernet Length

Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.

0: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).

1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).

Any: Any value is allowed ("don't-care").

IP

Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.

0: ARP/RARP frames where the HLD is not equal to Ethernet (1).

1: ARP/RARP frames where the HLD is equal to Ethernet (1).

Any: Any value is allowed ("don't-care").

Ethernet

Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.

0: ARP/RARP frames where the PRO is not equal to IP (0x800).

1: ARP/RARP frames where the PRO is equal to IP (0x800).

Any: Any value is allowed ("don't-care").

IPv4 Parameters

The IP parameters can be configured when Frame Type "IPv4" is selected.

IP Parameters

| | |
|--------------------|-----|
| IP Protocol Filter | Any |
| IP TTL | Any |
| IP Fragment | Any |
| IP Option | Any |
| SIP Filter | Any |
| DIP Filter | Any |

IP Protocol Filter

Specify the IP protocol filter for this ACE.

Any: No IP protocol filter is specified ("don't-care").

ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this section.

UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this section.

TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this section.

Other: If you want to filter another specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter displays.

IP Protocol Value

When "Other" is selected for the IP Protocol Filter (above), you can enter a specific value here. The valid range is **0** to **255**. A frame that hits this ACE matches this IP protocol value.

IP Parameters

| | |
|--------------------|-------|
| IP Protocol Filter | Other |
| IP Protocol Value | 1 |

IP TTL

Specify the Time-to-Live settings for this ACE.

Zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.

Non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.

Any: Any value is allowed ("don't-care").

IP Fragment

Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.

No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.

Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be

able to match this entry.

Any: Any value is allowed ("don't-care").

IP Option

Specify the options flag setting for this ACE.

No: IPv4 frames where the options flag is set must not be able to match this entry.

Yes: IPv4 frames where the options flag is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

SIP Filter

Specify the source IP filter for this ACE.

Any: No source IP filter is specified. (Source IP filter is "don't-care".)

Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.

Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

SIP Address

When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.

SIP Mask

When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation. The default is 255.255.255.0.

DIP Filter

Specify the destination IP filter for this ACE.

Any: No destination IP filter is specified. (Destination IP filter is "don't-care".)

Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.

Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.

DIP Address

When "Host" or "Network" is selected for the DIP Filter, you can enter a specific DIP address in dotted decimal notation.

DIP Mask

When "Network" is selected for the DIP Filter, you can enter a specific DIP mask in dotted decimal notation.

IPv6 Parameters

The IPv6 parameters can be configured when Frame Type "IPv6" is selected.

IPv6 Parameters

| | | |
|--------------------|-----|---|
| Next Header Filter | Any | ▼ |
| SIP Filter | Any | ▼ |
| Hop Limit | Any | ▼ |

Next Header Filter

Specify the IPv6 next header filter for this ACE.

Any: No IPv6 next header filter is specified ("don't-care").

ICMP: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this section.

UDP: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this section.

TCP: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this section.

other: If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears.

Next Header Value

When "**other**" is selected for the IPv6 next header value, you can enter a specific value. The allowed range is **0** to **255**. A frame that hits this ACE matches this IPv6 protocol value.

SIP Filter

Specify the source IPv6 filter for this ACE.

Any: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".)

specific: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.

SIP Address (32 bits)

When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address.

SIP BitMask (32 bits)

When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFF (bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.

Hop Limit

Specify the hop limit settings for this ACE.

0: IPv6 frames with a hop limit field greater than zero must not be able to match this entry.

1: IPv6 frames with a hop limit field greater than zero must be able to match this entry.

Any: Any value is allowed ("don't-care").

ICMP Parameters

ICMP Parameters

| | | |
|------------------|-----|---|
| ICMP Type Filter | Any | ▼ |
| ICMP Code Filter | Any | ▼ |

ICMP Type Filter

Specify the ICMP filter for this ACE.

Any: No ICMP filter is specified (ICMP filter status is "don't-care").

specific: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.

ICMP Type Value

When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is **0** to **255**. A frame that hits this ACE matches this ICMP value.

ICMP Code Filter

Specify the ICMP code filter for this ACE.

Any: No ICMP code filter is specified (ICMP code filter status is "don't-care").

specific: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.

ICMP Code Value

When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is **0** to **255**. A frame that hits this ACE matches this ICMP code value.

TCP Parameters

Source Port Filter

Specify the TCP/UDP source filter for this ACE.

Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").

Specific: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.

Range: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.

TCP Parameters

| | |
|--------------------|-----------|
| Source Port Filter | Range |
| Source Port Range | 0 - 65535 |
| Dest. Port Filter | Range |
| Dest. Port Range | 0 - 65535 |
| TCP FIN | Any |
| TCP SYN | Any |
| TCP RST | Any |
| TCP PSH | Any |
| TCP ACK | Any |
| TCP URG | Any |

Source Port No.

When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

TCPv6 Parameters

| | |
|--------------------|-----|
| Source Port Filter | Any |
| Dest. Port Filter | Any |
| TCP FIN | Any |
| TCP SYN | Any |
| TCP RST | Any |
| TCP PSH | Any |
| TCP ACK | Any |
| TCP URG | Any |

Source Port Range

When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

Destination Port Filter

Specify the TCP/UDP destination filter for this ACE.

Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care").

Specific: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.

Range: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value displays.

Dest. Port No.

When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

Destination Port Range

When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

TCP FIN

One of several TCP flag names used only when filtering TCP (*urg, ack, psh, rst, syn, and fin*). Specify the TCP "No more data from sender" (FIN) value for this ACE.

0: TCP frames where the FIN field is set must not be able to match this entry.

1: TCP frames where the FIN field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP SYN

One of several TCP flag names used only when filtering TCP (*urg, ack, psh, rst, syn, and fin*). Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.

0: TCP frames where the SYN field is set must not be able to match this entry.

1: TCP frames where the SYN field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP RST

One of several TCP flag names used only when filtering TCP (*urg, ack, psh, rst, syn, and fin*). Specify the TCP "Reset the connection" (RST) value for this ACE.

0: TCP frames where the RST field is set must not be able to match this entry.

1: TCP frames where the RST field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP PSH

One of several TCP flag names used only when filtering TCP (*urg, ack, psh, rst, syn, and fin*). Specify the TCP "Push" function (PSH) value for this ACE.

0: TCP frames where the PSH field is set must not be able to match this entry.

1: TCP frames where the PSH field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP ACK

One of several TCP flag names used only when filtering TCP (*urg, ack, psh, rst, syn, and fin*). Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.

0: TCP frames where the ACK field is set must not be able to match this entry.

1: TCP frames where the ACK field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP URG

One of several TCP flag names used only when filtering TCP (*urg, ack, psh, rst, syn, and fin*). Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.

0: TCP frames where the URG field is set must not be able to match this entry.

1: TCP frames where the URG field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

UDP Parameters

Source Port Filter

Specify the TCP/UDP source filter for this ACE.

Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care").

Specific: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.

Range: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.

UDP Parameters

| | |
|--------------------|----------|
| Source Port Filter | Specific |
| Source Port No. | 0 |
| Dest. Port Filter | Range |
| Dest. Port Range | 0 65535 |

Source Port No.

When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

UDpv6 Parameters

| | |
|--------------------|----------|
| Source Port Filter | Range |
| Source Port Range | 0 65535 |
| Dest. Port Filter | Specific |
| Dest. Port No. | 0 |

Source Port Range

When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

Dest. Port Filter

When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

Destination Port Range

When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

Ethernet Type Parameters

The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

EtherType Filter

Specify the Ethernet type filter for this ACE.

Any: No EtherType filter is specified (EtherType filter status is "don't-care").

Specific: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.

Ethernet Type Parameters

| | |
|------------------|------------|
| EtherType Filter | Specific ▾ |
| EtherType Value | 0xffff |

Ethernet Type Value

When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value.

The allowed range is **0x600** to **0xFFFF** but excludes 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6).

A frame that hits this ACE matches this EtherType value.

Bandwidth Profile using ACE (Access Control Entry)

Apart from MEF specified layer-2 services, the S4224 can associate the bandwidth profile parameters of < CIR, CBS, EIR, EBS, CM, CF> with any kind of traffic flow. The web interface provides the option of Layer 2 to Layer 4 flows to be associated with a bandwidth profile. The flow can be characterized by different Layer 2-4 options together and rules can be assigned to such a flow. One of the rules can be bandwidth. A sample screen for a TCP flow over a VLAN on Port 2 is shown below:

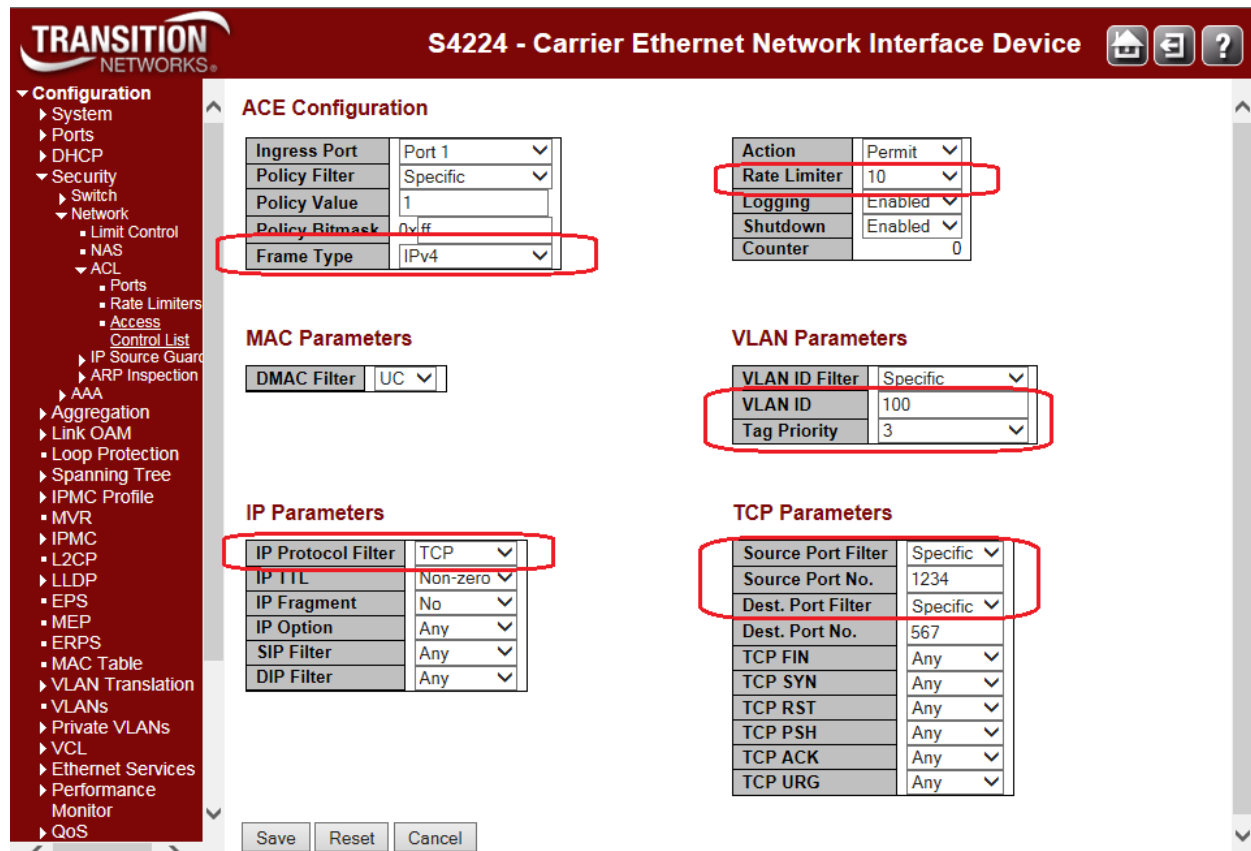


Figure 11: ACE for Flow-based BWP

IP Source Guard Configuration

IP Source Guard is a security feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

IP source guard checks the IP source address and MAC source address in a packet sent from a host attached to an untrusted access interface on the switch against entries stored in the DHCP snooping database. If IP source guard determines that the packet header contains an invalid source IP address or source MAC address, it ensures that the switch does not forward the packet (i.e., the packet is discarded). When you configure IP source guard, you enable on it on one or more VLANs. IP source guard applies its checking rules to packets sent from untrusted access interfaces on those VLANs.

After the DHCP snooping database is populated (via either dynamic DHCP snooping or configuring specific static IP address/MAC address bindings) the IP source guard database is built. It then checks incoming packets from access interfaces on the VLANs on which it is enabled. If the source IP addresses and source MAC addresses match the IP source guard binding entries, the switch forwards the packets to their specified destination addresses. If they do not match, the packets are discarded.

The **Configuration > Security > Network > IP Source Guard** menu path provides Configuration and Static table configuration.

The screenshot displays the web interface for configuring IP Source Guard on a Transition Networks S4224 device. The left-hand navigation menu is expanded to show the 'IP Source Guard' configuration options. The main configuration area is titled 'IP Source Guard Configuration' and features a 'Mode' dropdown menu currently set to 'Disabled'. Below this is a 'Translate dynamic to static' button. The 'Port Mode Configuration' section contains a table with the following data:

| Port | Mode | Max Dynamic Clients |
|------|----------|---------------------|
| 1 | Disabled | Unlimited |
| 2 | Disabled | Unlimited |
| 3 | Disabled | Unlimited |
| 4 | Disabled | Unlimited |
| 5 | Disabled | Unlimited |
| 6 | Disabled | Unlimited |
| 7 | Disabled | Unlimited |

The IP Source Guard Configuration table parameters are explained below.

IP Source Guard > Configuration

Here you can configure IP Source Guard Mode and Port Mode, and translate all dynamic entries to static entries for both ARP Inspection and Dynamic ARP Inspection. It is also possible to add a new entry to the Static ARP Inspection table and/or IP Source Guard by specifying the Port, VLAN ID, MAC address, and IP address for the new entry.

Mode

Enable or disable the Global IP Source Guard globally. All configured ACEs will be lost when the mode is enabled globally here. The * in the Port column acts as a 'wild card' character which causes the selections in this row to be applied to all other rows in the table for which this selection is valid.

Port Mode Configuration

Port

The Port column specifies if IP Source Guard is enabled on each port.

Mode

The table specifies if IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

Max Dynamic Clients

Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or **Unlimited**. If the Port mode is 'Enabled' and the value of 'Max Dynamic Clients' is equal to 0, it means to only allow the IP packets forwarding that are matched in static entries on the specific port. The default is **Unlimited**.

Buttons

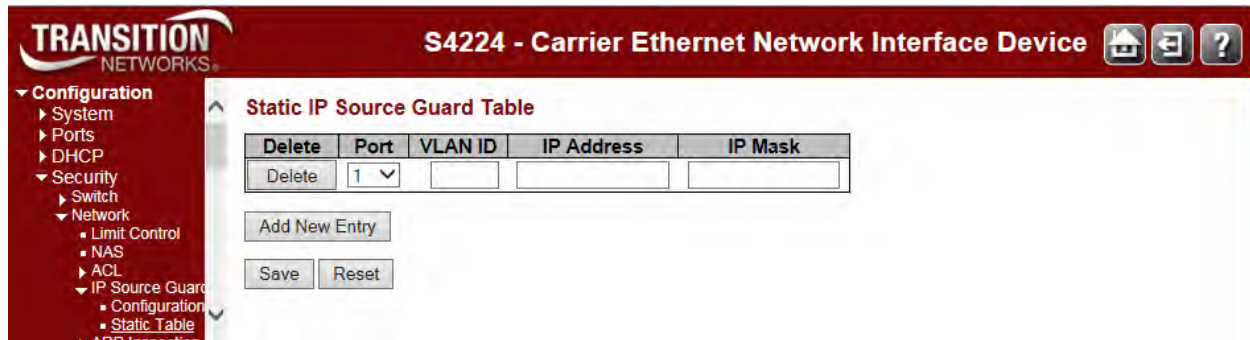
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Translate dynamic to static: Click to translate all dynamic entries to static entries. The IP Source Guard Configuration Mode must be set to Enabled, and an entry must exist in the Static IP Source Guard Table.

IP Source Guard > Static Table

The default Static IP Source Guard Table displays no saved entries. When you click the **Add New Entry** button, initial entry fields display.



The Static IP Source Guard Table parameters are described below.

Delete

Check to delete an existing entry. It will be deleted during the next save.

Port

The logical port for the settings. Select a port from the dropdown.

VLAN ID

Enter the VLAN ID for the settings.

IP Address

Enter the allowed Source IP address (e.g., enter *192.168.1.30*).

IP Mask

The IP Mask can be used for calculating the allowed network with IP address. A valid IP Mask is a dotted decimal string ('x.y.z.w'), where 1) x, y, and z are decimal numbers between 0 and 255, 2) when converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero.

Add New Entry

Click the **Add New Entry** button to add a new entry to the 'Static IP Source Guard' table. Specify the Port, VLAN ID, IP address, and IP Mask for the new entry. Click the **Save** button when done.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Example

The Static IP Source Guard Table shown below shows four new saved entries.

The screenshot shows the web interface for a Transition Networks S4224 - Carrier Ethernet Network Interface Device. The left sidebar shows the configuration menu with 'IP Source Guard' expanded to 'Static Table'. The main content area displays the 'Static IP Source Guard Table' with the following data:

| Delete | Port | VLAN ID | IP Address | IP Mask |
|--------------------------|------|---------|---------------|---------------|
| <input type="checkbox"/> | 1 | 10 | 192.168.1.30 | 255.255.255.0 |
| <input type="checkbox"/> | 1 | 10 | 192.168.1.210 | 255.255.255.0 |
| <input type="checkbox"/> | 2 | 10 | 192.168.1.210 | 255.255.255.0 |
| <input type="checkbox"/> | 3 | 10 | 192.168.1.210 | 255.255.255.0 |
| <input type="checkbox"/> | 3 | 20 | 192.168.1.210 | 255.255.255.0 |

Below the table are buttons for 'Add New Entry', 'Save', and 'Reset'.

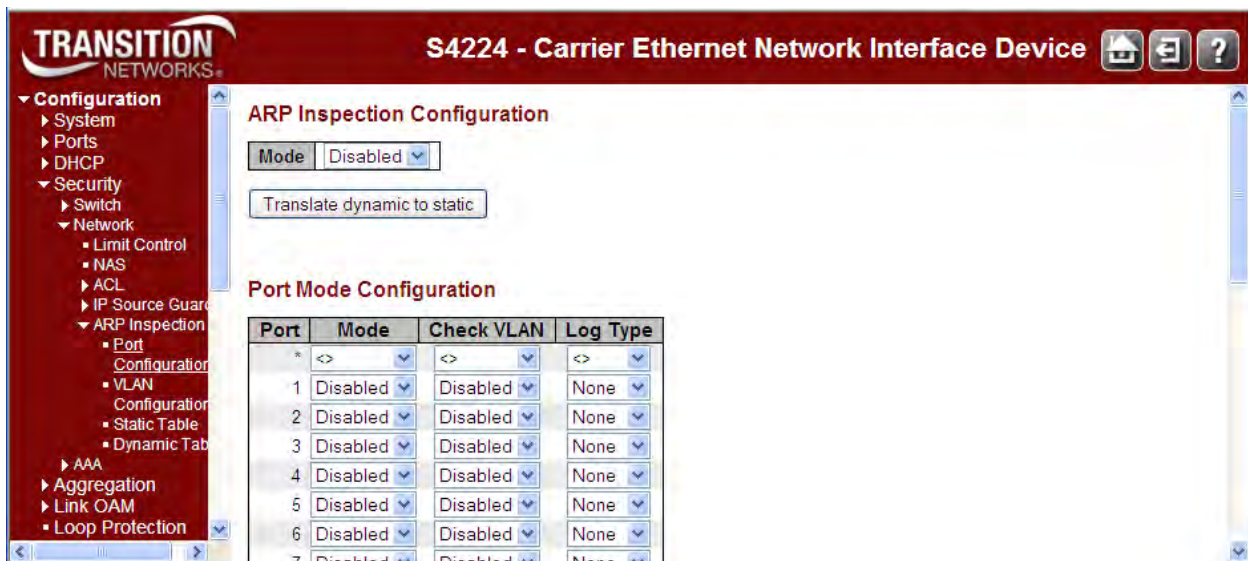
The example above has Port 1 with two entries with the same VLAN ID, different IP Addresses, and different MAC address. Port 3 has two entries for two different VLAN IDs with the same IP Address, and the same MAC address.

ARP Inspection Configuration

ARP Inspection is a security feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. The ARP Inspection feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Port Configuration

The **Configuration > Security > Network > ARP Inspection > Port Configuration** menu path provides global ARP Inspection configuration and Port level ARP Inspection configuration.



The ARP Inspection parameters are explained below.

ARP Inspection Configuration Mode

Enable or disable the Global ARP Inspection feature.

Port Mode Configuration

Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:

Enabled: Enable ARP Inspection operation.

Disabled: Disable ARP Inspection operation.

To inspect the VLAN configuration, enable the "**Check VLAN**" setting. The default setting of "Check VLAN" is disabled. Possible "Check VLAN" settings are:

Enabled: Enable check VLAN operation. When "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting.

Disabled: Disable check VLAN operation. When "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting.

If only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. The log types are:

None: Log nothing.

Deny: Log denied entries.

Permit: Log permitted entries.

ALL: Log all entries.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Translate dynamic to static: Click to translate all dynamic entries to static entries.

VLAN Configuration

The **Configuration > Security > Network > ARP Inspection > VLAN Configuration** menu path provides ARP Inspection related configuration. ARP Inspection is a security feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

From the default page, click the **Add New Entry** button to display the config table.

Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The " Start from VLAN " input field let you select the starting point in the VLAN Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next VLAN Table match. The **>>** button will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning message is shown in the displayed table. Use the **<<** button to start over.

VLAN Mode Configuration

Delete

Check to delete the entry. It will be deleted during the next save.

VLAN ID

The VLAN ID (VID) for these settings. Specify whether ARP Inspection is to be enabled on which VLANs. First, you must enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on the VLAN Mode Configuration page.

Log Type

You can configure the log type on a per-VLAN basis from the Log Type dropdown. Log Types are:

- None:** Log nothing.
- Deny:** Log denied entries.
- Permit:** Log permitted entries.
- All:** Log all entries.

Buttons

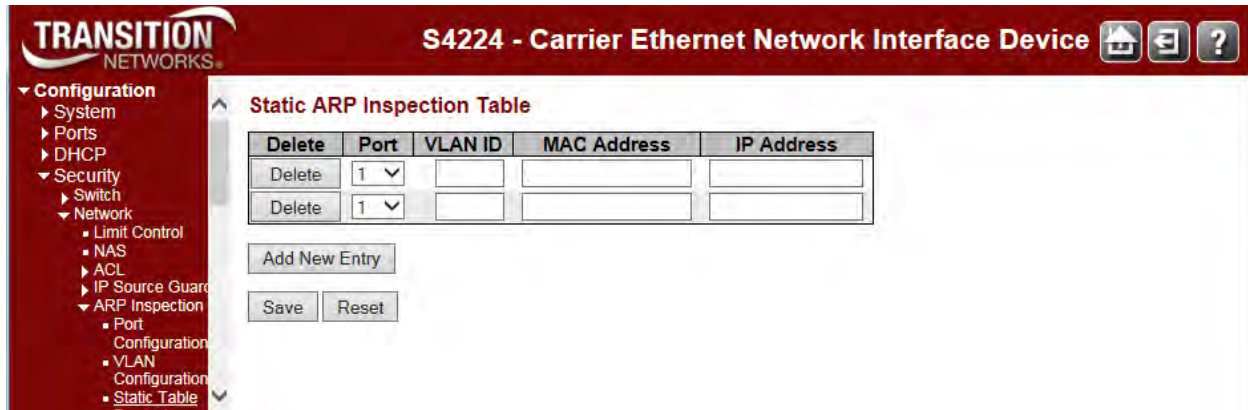
Add New Entry: Click to add a new VLAN to the ARP Inspection VLAN table.

Save: Click to save changes. You can add multiple new entries per Save operation.

Reset: Click to undo any changes made locally and revert to previously saved values.

Static ARP Inspection

The **Configuration > Security > Network > ARP Inspection > Static Table** menu path provides the default Static ARP Inspection **rules**. The switch supports a maximum of 256 rules. Click the **Add New Entry** button to display the entry table.



The Static ARP Inspection Table parameters are explained below.

Delete

Check to delete the entry. It will be deleted during the next save.

Port

The logical port for the settings.

VLAN ID

The VLAN ID (VID) for the settings.

MAC Address

Allows Source MAC address in ARP request packets (e.g., enter 00-c0-f2-56-08-b0).

IP Address

Allows Source IP address in ARP request packets.

Add New Entry

Click to add a new entry to the Static ARP Inspection table. Specify the Port, VLAN ID, MAC address, and IP address for the new entry. Click "Save" when done.

Buttons

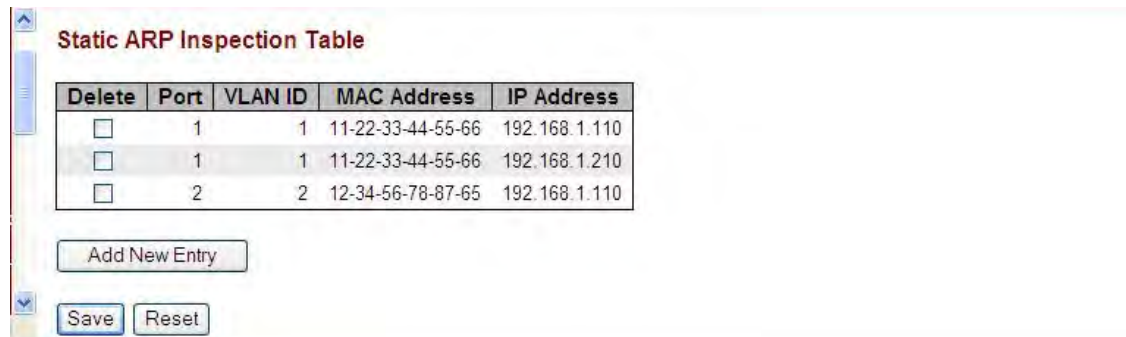
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Add New Entry: Click to add a new entry to the Static ARP Inspection table. See above.

Example

The Static ARP Inspection Table shown below shows three saved entries.



| Delete | Port | VLAN ID | MAC Address | IP Address |
|--------------------------|------|---------|-------------------|---------------|
| <input type="checkbox"/> | 1 | 1 | 11-22-33-44-55-66 | 192.168.1.110 |
| <input type="checkbox"/> | 1 | 1 | 11-22-33-44-55-66 | 192.168.1.210 |
| <input type="checkbox"/> | 2 | 2 | 12-34-56-78-87-65 | 192.168.1.110 |

Add New Entry

Save Reset

Note that you can create multiple entries and then Save them in one Save operation. You can also cut and paste information between fields. Use the keyboard Tab key to move from one field to the next.

Dynamic ARP Inspection

The **Configuration > Security > Network > ARP Inspection > Dynamic Table** menu path displays the Dynamic ARP Inspection Table. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learned from DHCP Snooping.

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The **>>** button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the **<<** button to start over.

Port

The logical port for the settings. This is the Switch Port Number for which the entries are displayed.

VLAN

The VLAN ID (VID) for the settings. This is the VLAN-ID in which the ARP traffic is permitted.

MAC Address

Allows Source MAC address in ARP request packets (e.g., enter 00-c0-f2-56-08-b0). This is the User MAC address of the entry.

IP Address

Allows Source IP address in ARP request packets. This is the User IP address of the entry.

Translate to static

Select the checkbox to translate the entry to static entry.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the input fields.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

|<< : Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

AAA Security Configuration

This page lets you configure the AAA (Authentication, Authorization and Accounting) Servers. You can configure the optional RADIUS and/or TACACS+ servers from the **Configuration > Security > AAA** menu path.

RADIUS (Remote Authentication Dial In User Service) networking protocol provides centralized access, authorization and accounting management for computers to connect and use a network service. RADIUS is a client/server system that keeps the authentication information for users, remote access servers, VPN gateways, and other resources in one central database.

TACACS+ (Terminal Access Controller Access Control System Plus) networking protocol provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Caution: Before enabling **RADIUS** or **TACACS+**, make sure that the related AAA server is operational and that at least the AAA server's IP address/hostname and encryption/decryption parameters are set correctly. Make sure using the following safe method:

1. Open a CLI session.
2. Enter the command "**security aaa con**".
3. Try to open a TELNET session.

Now, if the attempt fails (possibly because of an incorrect AAA parameter setting) access to the CLI agent is retained (via the CLI session) and any AAA parameter setting can be corrected in the CLI session.

Note that "RADIUS-Assigned QoS" and "RADIUS-Assigned VLAN" can be enabled and disabled on a per-port basis on the Network Access Server Configuration page via the **Configuration > Network > Security > NAS** menu path.

Config > Security > AAA > RADIUS

The RADIUS Server Configuration page lets you configure RADIUS Global and Server configuration. Click the **Add New Server** button to display the new RADIUS server config parameters.

RADIUS Server Configuration

Global Configuration

| | | |
|------------------|----------------------|---------|
| Timeout | 5 | seconds |
| Retransmit | 3 | times |
| Deadtime | 0 | minutes |
| Key | <input type="text"/> | |
| NAS-IP-Address | <input type="text"/> | |
| NAS-IPv6-Address | <input type="text"/> | |
| NAS-Identifier | <input type="text"/> | |

Server Configuration

| Delete | Hostname | Auth Port | Acct Port | Timeout | Retransmit | Key |
|--------|----------------------|-----------|-----------|----------------------|----------------------|----------------------|
| Delete | <input type="text"/> | 1812 | 1813 | <input type="text"/> | <input type="text"/> | <input type="text"/> |

Global Configuration

These settings are common for all of the RADIUS servers.

Timeout

The number of seconds, in the range **1** to **1000**, to wait for a reply from a RADIUS server before retransmitting the request.

Retransmit

Retransmit is the number of times, in the range **1** to **1000**, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.

Deadtime

Deadtime, which can be set to a number between **0** to **1440** minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than **0** (zero) will enable this feature, but only if more than one server has been configured.

Key

The secret key - up to 63 characters long - shared between the RADIUS server and the switch. The authentication messages sent to and from the RADIUS server use an authentication key, not a password. This authentication key, or shared secret, must be the same on the RADIUS client and server. Without this key, there is no communication between the client and server.

NAS-IP-Address (Attribute 4)

The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used. Must be a valid IP v4 address in dotted decimal notation (“x.y.z.w”), where x, y, z, and w are decimal numbers between 0 and 255.

NAS-IPv6-Address (Attribute 95)

The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used. Must be a valid IPv6 address in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon (:) separating each field.

NAS-Identifier (Attribute 32)

The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Server Configuration

The table has one row for each RADIUS server and a number of columns, which are:

Delete

To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.

Hostname

The IP address or hostname of the RADIUS server. Must be unique if configuring multiple servers.

Auth Port

The UDP port to use on the RADIUS server for authentication. Must be unique if configuring multiple servers.

Acct Port

The UDP port to use on the RADIUS server for accounting. Must be unique if configuring multiple servers.

Timeout

This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Retransmit

This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

Key

This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Add New Server Click to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported. The **Delete** button can be used to undo the addition of the new server.

Config > Security > AAA > TACACS+

This page lets you configure the TACACS+ server(s) and global parameters. Click the **Add New Server** button to add an empty row to the table.

Global Configuration

These settings are common for all of the TACACS+ servers.

Timeout

Timeout is the number of seconds, in the range **1** to **1000**, to wait for a reply from a TACACS+ server before it is considered to be dead.

Deadtime

Deadtime, which can be set to a number between **0** to **1440** minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the Deadtime to a value greater than **0** (zero) will enable this feature, but only if more than one server has been configured.

Key

The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Configuration

The table has one row for each TACACS+ server and a number of columns, which are:

Delete

To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.

Hostname

The IP address or hostname of the TACACS+ server.

Port

The TCP port to use on the TACACS+ server for authentication.

Timeout

This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Key

This optional setting overrides the global key. Leaving it blank will use the global key.

Adding a New Server

Click the **Add New Server** button to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported. The **Delete** button can be used to undo the addition of the new server.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Aggregation Configuration

Link aggregation (AKA trunking, link bundling, or Ethernet NIC bonding) are various methods of combining (aggregating) multiple network connections in parallel to increase throughput over that which a single connection could sustain, while providing redundancy in case one of the links fails.

Link aggregation addresses two Ethernet connection problems: bandwidth limitations and lack of resilience.

The S4224 supports both Static aggregation and LACP. Note that Aggregation mismatch can occur if the aggregation type on each end of the link does not match. Some switches do not implement the 802.1AX standard but support static link aggregation. Link aggregation between similarly 'statically' configured switches will work, but will fail between a statically configured switch and a device that is configured for LACP.

Link aggregation bundles multiple ports (member ports) together into a single logical link. It is used mainly to increase available bandwidth without introducing loops into the network, and to improve resilience against faults. A link aggregation group (LAG) can be established with individual links being dynamically added or removed. This enables bandwidth to be incrementally scaled based on changing requirements. A LAG can be quickly reconfigured if faults are identified.

Frames destined for a LAG are sent on only one of the LAGs member ports. The member port on which a frame is forwarded is determined by a 4-bit aggregation code (AC) that is calculated for the frame. The aggregation code ensures that frames belonging to the same frame flow (e.g., a TCP connection) are always forwarded on the same LAG member port. For that reason, reordering of frames within a flow is not possible. The AC is based on the following information:

1. SMAC (Source MAC address)
2. DMAC (Destination MAC address)
3. Source and Destination IPv4 address
4. Source and Destination TCP/UDP ports for IPv4 packets
5. Source and Destination TCP/UDP ports for IPv6 packets
6. IPv6 Flow Label

For best traffic distribution among LAG member ports, enable all six contributions to the AC.

Each LAG can consist of up to 16 member ports. Any quantity of LAGs may be configured for the S4224 (only limited by the number of device ports). To configure a proper traffic distribution, the ports within a LAG must use the same link speed.

A port cannot be a member of multiple LAGs.

The Aggregation Configuration parameters are explained below.

Static Aggregation

This page is used to configure the Aggregation hash mode and the aggregation group from the **Configuration > Aggregation > Static** menu path.

Aggregation involves using multiple ports in parallel to increase the link speed beyond the limits of a port, and to increase the redundancy for higher availability (aka 'Port Aggregation' or 'Link Aggregation').

Guidelines for Static Aggregation:

- A static aggregation can contain up to eight ports.
- All ports of a static aggregation must be of the same medium type (all twisted-pair ports or all fiber optic ports, but not a combination of the two).
- The aggregation ports can be either consecutive (e.g., Ports 2 - 4) or non-consecutive (e.g., ports 1, 3, and 5).
- Before creating a port aggregation, verify that the settings are the same for all ports in the trunk including speed, duplex mode, flow control, VLAN membership, etc. If these settings are not the same, the switch will not let you create the aggregation.
- After you create a port aggregation, a change to the speed, duplex mode, flow control, or back pressure of any port in the trunk automatically implements the same change on all the other member ports.
- A port can belong to only one static aggregation at a time.
- The ports of a static aggregation can be configured to be members of more than one VLAN.
- The ports of a static aggregation can be either tagged or untagged members of the same VLAN.

The default **Configuration > Aggregation > Static** page is shown below.

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

Configuration

- System
- Ports
- DHCP
- Security
- Aggregation
 - Static
 - LACP
- Link OAM
- Loop Protection
- Spanning Tree
- IPMC Profile
- MVR
- IPMC
- L2CP
- LLDP
- SyncE
- EPS
- MEP
- ERPS
- MAC Table
- VLAN Translation
- VLANs
- Private VLANs
- VCL

Aggregation Mode Configuration

| Hash Code Contributors | |
|-------------------------|-------------------------------------|
| Source MAC Address | <input checked="" type="checkbox"/> |
| Destination MAC Address | <input type="checkbox"/> |
| IP Address | <input checked="" type="checkbox"/> |
| TCP/UDP Port Number | <input checked="" type="checkbox"/> |

Aggregation Group Configuration

| Group ID | Port Members | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| Normal | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

The static aggregation parameters are explained below.

Aggregation Mode Configuration - Hash Code Contributors

Aggregation is possible based on hash values computed from fields in the frame. At least one of the hash code contributors checkboxes must be checked.

Source MAC Address

The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled as a hash code contributor.

Destination MAC Address

The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled as a hash code contributor.

IP Address

The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled as a hash code contributor.

TCP/UDP Port Number

The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled as a hash code contributor.

Aggregation Group Configuration

Group ID

Indicates the group ID for the settings contained in the same row. Group ID **Normal** indicates there is no aggregation. Only one group ID is valid per port.

Port Members

Each S4224 port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be of the same speed in each group. Each local aggregation group must contain 2 - 6 members.

Static aggregation cannot be enabled on ports whose 802.1X Admin State is not 'Authorized'. To configure the Spanning Tree function, see **Configuration > Spanning Tree > CIST Ports > CIST Normal Port Configuration** in the "STP Enabled" column.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Messages:

At least one hash code must be chosen

Aggregation Error - LACP aggregation is enabled

Aggregation Error - Port joining aggregation must be in the same speed and in full duplex

Aggregation Error - Static aggregation cannot be enabled on ports whose 802.1X Admin State is not Authorized

Group x member counts error!! - Local aggregation must include 2-6 ports.

LACP Error - LACP and Static aggregation can not both be enabled on the same ports

The aggregation must include 2-8 ports

Message: For GLAGs, port speed must match group speed and duplex must be full:

Half duplex ports are not allowed to join aggregation groups.

Port joining aggregation must be in the same speed and in full duplex

Port speed must be the same for all GLAG members. Port %lu removed from group.

Meaning: Glags do not exist or ok. Port speed must match group speed. Port joining aggregation must be in full duplex

Recovery: Verify that all ports are FDX and same speed.

The S4224 does not allow ports with different speeds and half duplex to be aggregated.

1. At **Configuration > Ports > Configuration**, configure Ports at identical speeds and also as Full Duplex.

2. At **Configuration > Aggregation > Static**, group ports with identical speeds and full duplex modes.

An Aggregation Error (see below) displays. Note that no error is displayed prior to version 2.1.3.

LACP (Link Aggregation Control Protocol)

This page is used to configure the [Aggregation](#) hash mode and the aggregation group from **Configuration > Aggregation > LACP**. The Link Aggregation Control Protocol (LACP) is an IEEE 802.3ad standard that allows bundling several physical ports together to form a single logical port.

The S4224 supports Link aggregation per IEEE 802.1AX-2008. The Link aggregation supports several physical links bundled into a single logical link for resiliency and load sharing. The S4224 uses LACP PDUs to negotiate with peer devices and to exchange information about the links to be bundled automatically when enabled on the physical port.

The resolved aggregation status and peer information status are available. The load sharing mechanism uses all the physical links to transfer the traffic, but for a flow only one link can be used to make sure the packets are sent/received in order. It uses a hash function to determine which port should carry a traffic flow. The device lets you choose the fields that are needed for generating the hash code needed for routing a flow through a single physical port belonging to the aggregate group.

LACP takes care of link failures where if one link fails the flows belonging to that link are transferred to another link based on the hash mechanism which needs to choose from the available links. The static aggregation option is also supported so the S4224 will work with devices which don't support LACP.

LACP works by sending frames (LACPDUs) down all links that have the protocol enabled. If it finds a device on the other end of the link that also has LACP enabled, it will also independently send frames along the same links enabling the two units to detect multiple links between themselves and then combine them into a single logical link. LACP can be configured in one of two modes: active or passive. In active mode it will always send frames along the configured links. In passive mode however, it acts as "speak when spoken to", and therefore can be used as a way of controlling accidental loops (as long as the other device is in active mode).

LACP has advantages over static configuration. For instance, with failover when a link fails and there is another device such as a Media Converter between the devices, which means that the peer will not see the link down. With static link aggregation the peer would continue sending traffic down the link causing it to be lost. The device can confirm that the configuration at the other end can handle link aggregation. With Static link aggregation, a cabling or configuration mistake could go undetected and cause undesirable network behavior.

Guidelines for creating LACP aggregations:

- The LACP module can have a maximum of 3 groups (number of ports / 2), and up to 6 ports can be in a LAG (Link Aggregation Group) at any time.
- LACP must be activated on both the S4224 and its partner device.
- The other device must be 802.3ad-compliant.
- The ports of an aggregate trunk must be the same medium type (all TP ports or all fiber ports).
- Aggregation ports can be consecutive (e.g., ports 1-5) or nonconsecutive (e.g., ports 2, 4, 6).
- A port can belong to only one LACP aggregator at a time.
- A port cannot be a member of an LACP aggregator and a static aggregation concurrently.
- The ports of an aggregate trunk must be untagged members of the same VLAN.
- LACP trunking is not supported in half-duplex mode. Twisted-pair ports must be set to Auto-Negotiation or 1000 Mbps / full-duplex mode.
- 1000Base-X fiber optic ports must be set to full-duplex mode.
- Only ports that are members of an aggregator will transmit LACPDU packets.
- A member port of an aggregator functions as part of an aggregate trunk only if it receives LACPDU packets from the remote device. If it does not receive LACPDU packets, it functions as a normal Ethernet port (forwarding network traffic while continuing to transmit LACPDU packets).

- The port with the highest priority in an aggregate trunk carries broadcast packets and packets with an unknown destination.
- Before creating an aggregate trunk between a TN device and another vendor's device, refer to the vendor's documentation to determine the maximum number of active ports the device can support in a trunk. If less than eight, the maximum number for the S4224, assign the other vendor's device a higher system LACP priority than your S4224. This helps avoid a conflict between the devices if some ports are put in standby mode when the devices create the trunk.

The **Configuration > Aggregation > LACP** menu path is used to configure the Aggregation hash mode and the aggregation group from the LACP Port Configuration table. **Note:** LACP and Static aggregation can not both be enabled on the same ports at the same time.

The screenshot shows the web interface for an S4224 device. The left sidebar contains a navigation menu with options like System, Ports, DHCP, Security, Aggregation (Static, LACP), Link OAM, Loop Protection, Spanning Tree, IPMC Profile, MVR, IPMC, L2CP, LLD, and Spanning Tree. The main content area is titled 'LACP Port Configuration' and contains a table with the following data:

| Port | LACP Enabled | Key | Role | Timeout | Prio |
|------|--------------------------|------|--------|---------|-------|
| * | <input type="checkbox"/> | <> | <> | <> | 32768 |
| 1 | <input type="checkbox"/> | Auto | Active | Fast | 32768 |
| 2 | <input type="checkbox"/> | Auto | Active | Fast | 32768 |
| 3 | <input type="checkbox"/> | Auto | Active | Fast | 32768 |
| 4 | <input type="checkbox"/> | Auto | Active | Fast | 32768 |
| 5 | <input type="checkbox"/> | Auto | Active | Fast | 32768 |
| 6 | <input type="checkbox"/> | Auto | Active | Fast | 32768 |
| 7 | <input type="checkbox"/> | Auto | Active | Fast | 32768 |
| 8 | <input type="checkbox"/> | Auto | Active | Fast | 32768 |

This page lets you view and modify the following LACP port parameters.

Port

The S4224 port number. The * in the Port column acts as a 'wild card' character which causes the selections in this row to be applied to all other rows in the table for which this selection is valid.

LACP Enabled

Controls whether LACP is enabled on this S4224 port. LACP will form an aggregation when 2 or more ports are connected to the same partner. The S4224 can support up to four LAGs (assuming two ports in each LAG). LACP cannot be enabled on ports whose 802.1X Admin State is not Authorized. To configure the Spanning Tree function, use the **Configuration > Spanning Tree > CIST Ports > CIST Normal Port Configuration** menu path in the "STP Enabled" column.

Key

The **Key** value incurred by the port, range 1-65535. The **Auto** setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the **specific** setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot. The default is **Auto**.

Role

The **Role** shows the LACP activity status. The **Active** will transmit LACP packets each second, while **Passive** will wait for a LACP packet from a partner (i.e., 'speak if spoken to'). The default is **Active**.

Timeout

The **Timeout** controls the period between BPDU transmissions. **Fast** will transmit LACP packets each second, while **slow** will wait for 30 seconds before sending a LACP packet. The default is **Fast**.

Prio

The **Prio** controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. A lower number means a greater priority. The default is **32768**.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Messages:

LACP Error - LACP and Static aggregation can not both be enabled on the same ports

LACP Error - LACP cannot be enabled on ports whose 802.1X Admin State is not Authorized

Link OAM (LOAM) Configuration

The Ethernet Operations, Administration and Maintenance (OAM) protocol is used for monitoring and troubleshooting Ethernet networks.

The S4224 supports the OAM functionality in both point-to-point link monitoring as ascribed in IEEE 802.3ah and also Flow OAM requirements from IEEE 802.1ag as well as the IEEE standards, ITU-T G.1731 and ITU-T G.8021.

The S4224 supports Point-to-point link level OAM per 802.3ah to monitor the link operations in both Active and Passive mode. Mechanisms to support the following are implemented:

1. OAM capability Discovery.
2. Link monitoring: link events notifications with diagnostic information.
3. Software based Remote failure indication: to indicate a peer that receive path of the local DTE is non-operational.
4. Remote loop back control: a data link layer frame-level loop back mode.

You can enable or disable the OAM functionality depending on the topology requirements. These port-based configurations are supported:

1. Mode selection (active/passive)
2. OAM Client configuration for Capability Discovery Protocol and related timers.
3. Enable/Disable Link Monitoring capability once the Link Monitor capability is enabled, OAM entity sends out PDU with Link monitoring capability Flag set.
4. Enable/Disable Link monitoring operation; Link monitoring notifications are send out to the peer OAM entity only when the state of discovery protocol is "send-any" as defined by the IEEE 802.3ah.
5. Enable or disable the Remote loop back control capability; once the Remote loop back control capability is enabled, the OAM entity sends out PDU with Remote loop back capability Flag.
6. Enable or disable Remote loop back operation.

A Passive OAM entity obeys the remote loop back request from the peer OAM entity only when the state of the discovery protocol is "send-any" as defined by the IEEE 802.3ah. Note that IEEE 802.3ah does not specify the configuration support for most of these features.

S4224 Link OAM configuration involves 'Port Settings' and 'Event Settings' as explained below.

Link OAM Port Settings

This page lets you view and edit the current Link OAM port configurations from the **Configuration > Link OAM > Port Settings** menu path.

The screenshot shows the configuration interface for a S4224 device. The main title is "S4224 - Carrier Ethernet Network Interface Device". The left sidebar shows a navigation menu with "Configuration" expanded to "Link OAM" > "Port Settings". The main content area is titled "Link OAM Port Configuration" and contains a table with the following columns: Port, OAM Enabled, OAM Mode, Loopback Support, Link Monitor Support, MIB Retrieval Support, and Loopback Operation.

| Port | OAM Enabled | OAM Mode | Loopback Support | Link Monitor Support | MIB Retrieval Support | Loopback Operation |
|------|--------------------------|----------|--------------------------|-------------------------------------|--------------------------|--------------------------|
| * | <input type="checkbox"/> | <> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | <input type="checkbox"/> | Passive | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | Passive | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | Passive | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | Passive | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | Passive | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | Passive | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> | Passive | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> | Passive | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 9 | <input type="checkbox"/> | Passive | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 10 | <input type="checkbox"/> | Passive | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Port

The S4224 port number. Click on a specific port number in the table to display that port's 'Detailed Link OAM Status'. The * in the Port column acts as a 'wild card' character which causes the selections in this row to be applied to all other rows in the table for which this selection is valid. See the **Monitor > Link OAM > Port Statistics** section for more information.

OAM Enabled

Controls whether Link OAM is enabled on this S4224 port. Enabling Link OAM provides the network operator the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions.

OAM Mode

Configures the OAM Mode as **Active** or **Passive**. The default mode is **Passive**.

Active: DTEs configured in Active mode initiate the exchange of Information OAMPDUs as defined by the Discovery process. Once the Discovery process completes, Active DTEs are permitted to send any OAMPDU while connected to a remote OAM peer entity in Active mode. Active DTEs operate in a limited respect if the remote OAM entity is operating in Passive mode. Active devices should not respond to OAM remote loopback commands and variable requests from a Passive peer.

Passive: DTEs configured in Passive mode do not initiate the Discovery process. Passive DTEs react to the initiation of the Discovery process by the remote DTE. This eliminates the possibility of passive to passive links. Passive DTE will not send Variable Request or Loopback Control OAMPDUs.

Loopback Support

Controls whether the loopback support is enabled for the S4224 port. Link OAM remote loopback can be used for fault localization and link performance testing. Enabling the loopback support allows the DTE to execute the remote loopback command that helps in the fault detection.

Link Monitor Support

Controls whether the Link Monitor support is enabled for the S4224 port. On enabling the Link Monitor support, the DTE supports event notification that permits the inclusion of diagnostic information.

MIB Retrieval Support

Controls whether the MIB Retrieval Support is enabled for the S4224 port. On enabling MIB retrieval support, the DTE supports polling of various Link OAM based MIB variables' contents. Note that if MIB Retrieval Support is enabled, 'Loopback Operation' must be disabled. If both are enabled, the message "OAM Error - Error while configuring the OAM loopback" displays. To recover, click the browser's Back button and disable either MIB Retrieval Support or Loopback Operation.

Loopback Operation

If "Loopback Support" is enabled (see above), checking this checkbox will start a loopback operation for the port.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Messages:

OAM Error - Error while configuring the OAM loopback.

OAM Error - Error requested configuration is not supported with the current OAM mode

Link OAM Event Settings

This page lets you view and edit the current Link OAM port configurations from the **Configuration > Link OAM > Event Settings** menu path.

| Event Name | Error Window | Error Threshold |
|---------------------------|--------------|-----------------|
| Error Frame Event | 1 | 1 |
| Symbol Period Error Event | 1 | 1 |
| Seconds Summary Event | 60 | 1 |

Save Reset

The Link Event Configuration parameters are explained below.

Port x

The S4224 port number. The port select box determines which port is affected by clicking the buttons. The * in the Port column acts as a 'wild card' character which causes the selections in this row to be applied to all other rows in the table for which this selection is valid.

Event Name

Name of the Link Event which is being configured.

Error Window

Represents the window period in the order of **1** second for the observation of various link events.

Error Threshold

Represents the threshold value for the window period for the appropriate Link event so as to notify the peer of this error.

Error Frame Event

The Errored Frame Event counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of **1** second). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer.

Error Window for 'Error Frame Event' must be an integer value from **1** - **60** and its default value is '**1**'. Error Threshold must be between **0** - **0xffffffff** and its default value is '**0**'.

Symbol Period Error Event

The Errored Symbol Period Event counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period.

Error Window for 'Symbol Period Error Event' must be an integer value from **1** - **60** and its default value is '**1**'. Error Threshold must be between **0** - **0xffffffff** and its default value is '**1**'.

Seconds Summary Event

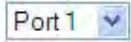
The Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is

generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a one second interval wherein at least one frame error was detected. Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer.

Error Window for 'Seconds Summary Event' must be an integer value from **10** - **900** and its default value is '**60**'.

Error Threshold must be between **0** - **0xffff** and its default value is '**1**'.

Buttons

: The port select box determines which port is affected by clicking the buttons.

Clear: Clears the counters for the selected port.

Save: Click to save changes.

Messages

Message: *OAM Error - Error While Configuring Link Events*

Message: *Unknown trap from OID: 1.3.6.1.2.1.158.*

Meaning: At **Link OAM > Event Settings**, if the Symbol Period Error Event - Error Threshold is set to 0, the message is continuously displayed on the CLI:

Recovery: Set the value to a non-zero value to stop the message.

Detailed Link OAM Status

After a 'Save', at the **Link OAM Port Configuration** page, click on a linked Port number in the "Port" column to display that particular port's "Detailed Link OAM Status" information.

Detailed Link OAM Status for Port 3 Port 3

| | |
|------------------|---------------|
| PDU Permission | Receive only |
| Discovery State | Passive state |
| Peer MAC Address | ----- |

| Local | Peer |
|--------------------------------------|------------|
| Mode | Passive |
| Unidirectional Operation Support | Disabled |
| Remote Loopback Support | Enabled |
| Link Monitoring Support | Disabled |
| MIB Retrieval Support | Enabled |
| MTU Size | 1500 |
| Multiplexer State | Forwarding |
| Parser State | Forwarding |
| Organizational Unique Identification | 00-c0-f2 |
| PDU Revision | 0 |

This page provides Link OAM configuration operational status. The displayed fields show the active configuration status for the selected port.

The fields are described below.

PDU Permission

Displays the port's current level of PDU permissions (e.g., **Info exchange**, **Receive only**).

Discovery State

Displays the port's current state of discovery (e.g., **Active state**, **Fault state**).

Peer MAC Address

Displays the peer's MAC address or "-----" if no peer is available.

Local and Peer

Mode

The Mode in which the Link OAM is operating; **Active** or **Passive**.

Unidirectional Operation Support

This feature is not user configurable. The status of this configuration is retrieved from the PHY (e.g., **Disabled** or **Disabled**).

Remote Loopback Support

If status is enabled, DTE is capable of OAM remote loopback mode (e.g., **Disabled** or **Disabled**).

Link Monitoring Support

If status is enabled, DTE supports interpreting Link Events (e.g., **Disabled** or **Disabled**).

MIB Retrieval Support

If status is enabled, DTE supports sending Variable Response OAMPDUs (e.g., **Disabled** or **Disabled**).

MTU Size

Represents the largest OAMPDU, in octets, supported by the DTE. This value is compared to the remote's Maximum PDU Size and the smaller of the two is used (e.g., 1500).

Multiplexer State

When **Forwarding** displays, the device is forwarding non-OAMPDUs to the lower sublayer. When **Discarding** displays, the device discards all the non-OAMPDUs.

Parser State

When **Forwarding** displays, the device is forwarding non-OAMPDUs to higher sublayer.
When **Loopback**, displays, the device is looping back non-OAMPDUs to the lower sublayer.
When **Discarding** displays, the device is discarding non-OAMPDUs.

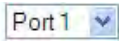
Organizational Unique Identification

Displays the 24-bit Organizationally Unique Identifier (OUI) of the vendor, if available (e.g., 00-01-c1).

PDU Revision

It indicates the current revision of the Information TLV. The value of this field starts at zero and be incremented each time something in the Information TLV changes. Upon reception of an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed (an Information TLV that is identical to the previous Information TLV does not need to be parsed as nothing in it has changed).

Buttons

: The **Port select box**: determines which port is affected.

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this checkbox to automatically refresh the page every three seconds. .

Note that the **Monitor > Link OAM** menu path provides LOAM **Statistics**, **Port Status**, and **Event Status** information.

Loop Protection Configuration

The **Configuration > Loop Protection** menu path lets you view and/or change the current global and port-level Loop Protection configuration.

Note: If you will be using the S4224 Loop Protection function, enable Loop Protection here, both globally and at the port level, as one of the first overall configuration steps.

Loop protection increases the efficiency of STP, RSTP, and MSTP by preventing ports from going into a forwarding state that would result in a loop opening up in the network. In spanning tree topologies, a loop-free network is supported by the exchange of a BPDU. Peer STP applications running on the switch interfaces use BPDUs to communicate. The exchange of BPDUs ultimately determines which interfaces block traffic (preventing loops) and which interfaces become root ports and forward traffic. However, a blocking interface can transition to the forwarding state erroneously if the interface stops receiving BPDUs from its designated port on the segment. This transition error can occur with a hardware error on the switch or a software configuration error between the switch and its neighbor.

With loop protection enabled, the spanning tree topology detects root ports and blocked ports, and ensures that both keep receiving BPDUs. If a loop protection enabled interface quits receiving BPDUs from its designated port, it reacts as it would react to a problem with the physical connection on this interface. Rather than transition the interface to a forwarding state, it instead transitions it to a 'loop inconsistent' state. The interface recovers, and then it transitions back to the spanning tree blocking state when it receives a BPDU.

Loop protection is most effective when enabled in the entire switched network. You should generally enable loop protection on all switch interfaces that could become a root or designated port. If you will be using the Loop Protection function, enable Loop Protection here, both globally and at the port level, as one of the first overall configuration steps.

The default screen is shown below.

The screenshot shows the web interface for the S4224 - Carrier Ethernet Network Interface Device. The main content area is titled "Loop Protection Configuration" and is divided into two sections: "General Settings" and "Port Configuration".

General Settings

| Global Configuration | |
|------------------------|-------------|
| Enable Loop Protection | Disable |
| Transmission Time | 5 seconds |
| Shutdown Time | 180 seconds |

Port Configuration

| Port | Enable | Action | Tx Mode |
|------|-------------------------------------|---------------|---------|
| * | <input checked="" type="checkbox"/> | <> | <> |
| 1 | <input checked="" type="checkbox"/> | Shutdown Port | Enable |
| 2 | <input checked="" type="checkbox"/> | Shutdown Port | Enable |
| 3 | <input checked="" type="checkbox"/> | Shutdown Port | Enable |
| 4 | <input checked="" type="checkbox"/> | Shutdown Port | Enable |
| 5 | <input checked="" type="checkbox"/> | Shutdown Port | Enable |
| 6 | <input checked="" type="checkbox"/> | Shutdown Port | Enable |
| 7 | <input checked="" type="checkbox"/> | Shutdown Port | Enable |
| 8 | <input checked="" type="checkbox"/> | Shutdown Port | Enable |

The Loop Protection parameters are explained below.

General Settings - Global Configuration

Enable Loop Protection

Controls whether loop protections is enabled (as a whole) or disabled.

Transmission Time

The interval between each loop protection PDU sent on each port. Valid values are **1** - **10** seconds.

Shutdown Time

The period (in seconds) for which a port will be kept disabled if a loop is detected (and the port action shuts down the port). Valid values are **0** to **604800** seconds (7 days). A value of zero (**0**) will keep a port disabled (until the next device restart).

Port Configuration

Port

The switch port number of the port. Note that loop protection is not supported on the MGMT/data port.

Enable

Controls whether loop protection is enabled on this S4224 port.

Action

Configures the action to be performed when a loop is detected on a port. The valid Actions are:

Sets the action to be performed when a loop is detected on a port. Valid loop protect Action values are:

Shutdown Port: Shutdown the port.

Shutdown and Log : Shutdown the port and Log the event.

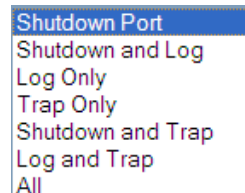
Log Only: Only Log the event.

Trap Only: Only send a trap.

Shutdown and Trap: Shutdown the port and Send trap.

Log and Trap: Send Trap and Log the event.

All: Shutdown the port, send trap, and Log the event.



Tx Mode

Controls whether the port is actively generating loop protection PDUs, or whether it is just passively looking for looped PDUs.

Enable: this port is actively generating loop protection PDUs.

Disable: this port is passively looking for looped PDUs.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Spanning Tree

The S4224 Spanning Tree menu provides the STP (Spanning Tree Protocol) configuration sub-menus from the **Configuration > Spanning Tree** menu path.

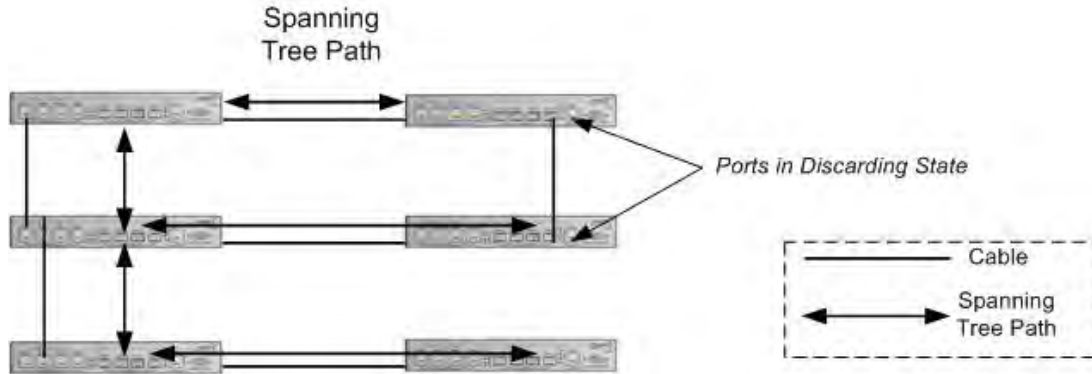


Figure 2. Spanning Tree Example

The Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop-free topology for any bridged LAN.

STP/RSTP/MSTP

The S4224 supports the spanning tree protocols of STP/RSTP and MSTP on all interfaces. The Spanning Tree protocols help in creating a loop free bridged network. The implementation conforms to the IEEE specs 802.1D for STP, 802.1w for RSTP and 802.1s for MSTP.

The S4224 can act in the role of a root bridge or as a designated bridge by the process of election. The priorities for the bridge instance that is used in BPDU frames can be configured. For MSTP, each MSTI (Multiple Spanning Tree Instance) priority can be configured for the Common and Internal Spanning Tree (CIST) instance.

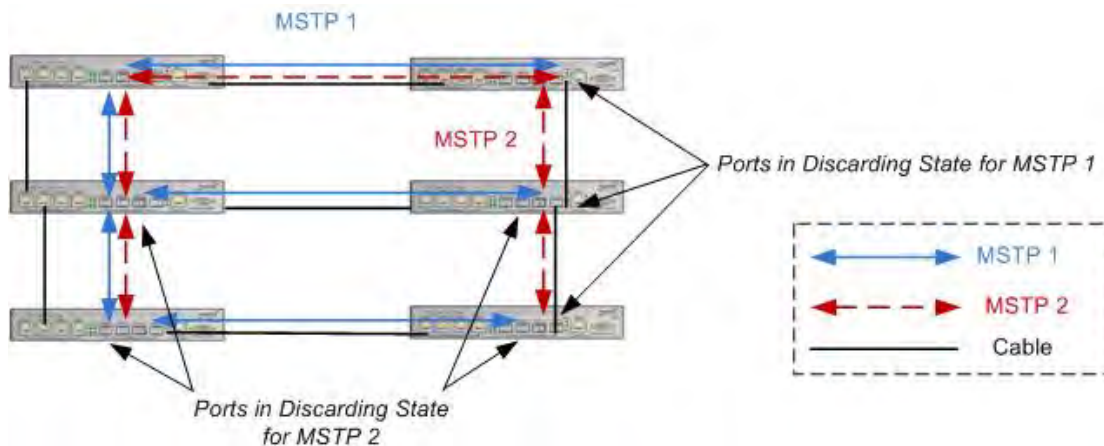
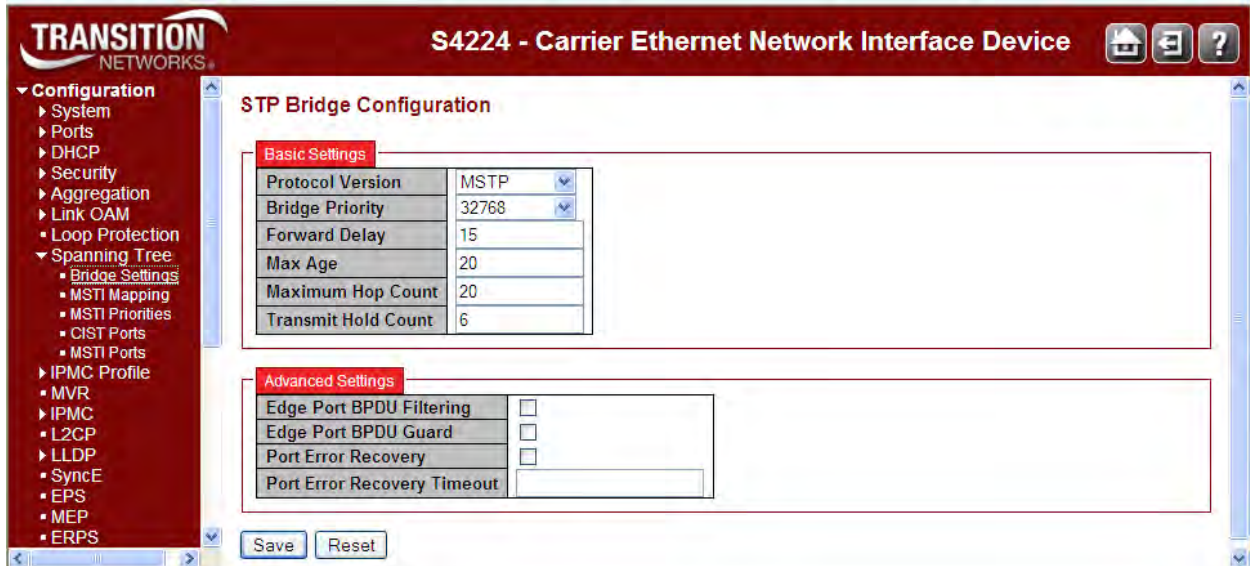


Figure 3. Multiple Spanning Tree Example

The Spanning Tree sub-menus (Bridge Settings, MSTI Mapping, MSTI Priorities, CIST Ports, and MSTI Ports) are described below.

Bridge Settings

S4224 STP Bridge configuration is done from the **Configuration > Spanning Tree > Bridge Settings** menu path.



This page lets you configure STP system settings, which are used by all S4224 STP Bridge instances.

Basic Settings

Protocol Version

The STP protocol version setting. Valid values are **STP**, **RSTP** and **MSTP**. The default is **MSTP**.

| Protocol Version | MSTP |
|------------------|------|
| | STP |
| | RSTP |
| | MSTP |

MSTP : MSTP (Multiple Spanning Tree Protocol) is an evolution of RSTP. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The IEEE 802.1Q-2005 standard, section 13 discusses MSTP. For MSTP details see <http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf>. MSTP works over VLAN instances, and multiple VLANs can be added to an MSTI; however, at any time a VLAN can only be part of one MSTI. Configuration for each MSTI and the VLANs that belong to that instance is supported. The S4224 also supports configuration of enabling/disabling BPDU guard, path cost for that port, restricting topology change notification, etc. Note that MSTP is disabled on the S4224 MGMT/data port.

RSTP: IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. The IEEE 802.1D-2004 standard now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP. The IEEE 802.1D-2004 standard, section 17 discusses RSTP. See <http://standards.ieee.org/getieee802/download/8021D-2004.pdf>. RSTP switch port states include Discarding (no user data is sent over the port), Learning (the port is not forwarding frames yet, but is populating its MAC-address-table), and Forwarding (the port is fully operational).

STP: Spanning Tree Protocol (STP) is an OSI layer-2 protocol that ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

Bridge Priority

Sets the bridge priority (the priority setting among other switches in the Spanning Tree). Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the S4224 forms a *Bridge Identifier*.

For **MSTP** operation, this is the priority of the CIST (Common and Internal Spanning Tree).

For **STP** or **RSTP** operation, this is the priority of the STP/RSTP bridge.

Select a Bridge Priority of 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, or 61440. The default is **32768**.

Forward Delay

The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range **4** to **30** seconds. The default is **15** seconds.

Max Age

The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are **6** - **40** seconds, and **Max Age** must be $\leq (\text{FwdDelay}-1)*2$. The default is **20** seconds.

Maximum Hop Count

This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to.

Valid values are **6** to **40** hops. The default is **20** hops.

Transmit Hold Count

The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range **1** to **10** BPDU's per second. The default is **6** BPDU's / second.

Advanced Settings

Edge Port BPDU Filtering

Control whether a port which is explicitly configured as **Edge** will transmit and receive BPDUs.

Edge Port BPDU Guard

Check the checkbox to force a port which is explicitly configured as **Edge** will disable itself upon reception of a BPDU. The port will enter the *error-disabled* state, and will be removed from the active topology.

Port Error Recovery

Check the checkbox to force a port in the *error-disabled* state to be automatically enabled after a certain time. If recovery is not enabled, ports must be disabled and then re-enabled for normal STP operation.

The condition is also cleared by a system reboot.

Port Error Recovery Timeout

The time to pass before a port in the *error-disabled* state can be enabled. Valid values are **30** - **86400** seconds (24 hours). The 'Port Error Recovery' checkbox (above) must be checked to be able to make an entry in this field.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

MSTI Mapping

MSTI (Multiple Spanning Tree Instance) configuration is done from the **Configuration > Spanning Tree > MSTI Mapping** menu path.

MSTP enables the grouping and mapping of VLANs to different spanning tree instances. An MSTI (MST Instance) is a particular set of VLANs that use the same spanning tree.

MSTI Configuration

Add VLANs separated by spaces or comma.
Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

| | |
|------------------------|-------------------|
| Configuration Name | 00-c0-f2-56-19-08 |
| Configuration Revision | 0 |

MSTI Mapping

| MSTI | VLANs Mapped |
|-------|--------------|
| MSTI1 | |
| MSTI2 | |
| MSTI3 | |
| MSTI4 | |
| MSTI5 | |
| MSTI6 | |
| MSTI7 | |

Save Reset

This page lets you view and/or edit the current STP MSTI bridge instance priority configurations.

Configuration Identification

Configuration Name

The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTIs (Intra-region). Enter a name of up to 32 characters.

Configuration Revision

The revision of the MSTI configuration named above. This must be an integer from 0 to 65535.

MSTI Mapping

MSTI

The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

VLANs Mapped

The list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to *one* MSTI. An unused MSTI should just be left empty (i.e., not have any VLANs mapped to it). Enter a single VLAN ID or a range of VLAN IDs. Note that VLAN 0 is invalid.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

MSTI Priorities

MSTI Priority Configuration is done from the **Configuration > Spanning Tree > MSTI Mapping** menu path.

| MSTI | Priority |
|-------|----------|
| * | 32768 |
| CIST | 32768 |
| MSTI1 | 32768 |
| MSTI2 | 32768 |
| MSTI3 | 32768 |
| MSTI4 | 32768 |
| MSTI5 | 32768 |
| MSTI6 | 32768 |
| MSTI7 | 32768 |

Save Reset

This page lets you view and/or edit the current STP MSTI bridge instance priority configurations.

MSTI

The bridge instance. The CIST is the *default* instance, which is always active. The * in the MSTI column acts as a 'wild card' character which causes the selections in this row to be applied to all other rows in the table for which this selection is valid.

Priority

Sets the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte S4224 MAC address forms a *Bridge Identifier*. Select 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, or 61440. The default is **32768**.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

CIST Ports

CIST (Common and Internal Spanning Tree) Port configuration is done from the **Configuration > Spanning Tree > CIST Ports** menu path.

The CIST is the default spanning tree instance of MSTP (i.e. all VLANs that are not members of particular MSTIs are members of the CIST). Also, an individual MST region can be regarded a single virtual bridge by other MST regions. The spanning tree that runs between regions is the CIST.

The screenshot shows the web interface for an S4224 Carrier Ethernet Network Interface Device. The main content area is titled "STP CIST Port Configuration" and contains two tables:

CIST Aggregated Port Configuration

| Port | STP Enabled | Path Cost | Priority | Admin Edge | Auto Edge | Restricted Role | TCN | BPDU Guard | Point-to-point |
|------|-------------------------------------|-----------|----------|------------|-------------------------------------|--------------------------|--------------------------|--------------------------|----------------|
| - | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Forced True |

CIST Normal Port Configuration

| Port | STP Enabled | Path Cost | Priority | Admin Edge | Auto Edge | Restricted Role | TCN | BPDU Guard | Point-to-point |
|------|-------------------------------------|-----------|----------|------------|-------------------------------------|--------------------------|--------------------------|--------------------------|----------------|
| * | <input checked="" type="checkbox"/> | <> | <> | <> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <> |
| 1 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 2 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 3 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 4 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 5 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 6 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 7 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 8 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |
| 9 | <input checked="" type="checkbox"/> | Auto | 128 | Non-Edge | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Auto |

This page lets you view and/or edit the current STP CIST port configurations and contains settings for physical (Normal) and aggregated ports.

Point-to-Point and Edge Ports selections apply to RSTP only. Part of the task of configuring RSTP is defining the port types on the bridge, which is directly related to the device(s) connected to the port. With the port types defined, RSTP can reconfigure a network much quicker than STP when a change in network topology is detected. The two possible selections are **Non-Edge** (Point-to-point) port or **Edge** port.

If a bridge port is connected to another bridge or router port, it normally operates in full-duplex mode and is functioning as a point-to-point port.

A port operates as an edge port when it is connected to a network terminal device such as a workstation or a server. An edge port on a bridge should not have any STP or RSTP devices connected to it either directly or through another device connected to that port. In this configuration since the port has no STP or RSTP devices connected to it, it will always forward network traffic.

Port

The S4224 port number of the logical STP port. The * in the Port column acts as a 'wild card' character which causes the selections in this row to be applied to all other Ports (rows) in the table for which this selection is valid.

STP Enabled

Controls whether STP is enabled on this S4224 port. Note that STP on MGMT / Port 1 is disabled by default.

Path Cost

Controls the path cost incurred by the port (dropdown and entry field).

The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. This is the default setting.

The **specific** setting lets you define the Path Cost value in the entry box. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range of 1 to 200,000,000. If **specific** is selected at the dropdown, you must enter a Path Cost value in the entry field.

Priority

Controls the port priority. This can be used to control priority of ports having identical Path Costs (see above). Select 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, or 240. The default is **128**.

operEdge (state flag)

Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having *operEdge true*) than for other ports. The value of this flag is based on Admin Edge and Auto Edge fields. This flag is displayed as **Edge** in **Monitor > Spanning Tree > STP Detailed Bridge Status**.

AdminEdge

Controls whether the *operEdge* flag should start as set or cleared. (The initial *operEdge* state when a port is initialized). Select **Edge** or **Non-Edge**. The default is **Edge**.

AutoEdge

Controls whether the bridge should enable automatic edge detection on the bridge port. This allows *operEdge* to be derived from whether BPDUs are received on the port or not. The default is automatic edge detection on the bridge port enabled (checkbox checked).

Restricted Role

If checked, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as **Root Guard**. The default is unchecked.

Restricted TCN

If checked, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state that the attached LANs transits frequently. The default is unchecked.

BPDU Guard

If checked, causes the port to disable itself upon receiving valid BPDUs. Contrary to the similar bridge setting, the port **Edge** status does not affect this setting. The default is unchecked.

A port entering error-disabled state due to this setting is subject to the bridge 'Port Error Recovery' setting as well. See the "Port Error Recovery" field description in the "**Bridge Settings**" section on page [158](#).

BPDU Guard is provided as part of the STP Configuration advanced global bridge settings. It controls whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology. It should be noted that there is also a (CIST) port setting for the BPDU Guard as mentioned above. This is not subject to "Edge" status dependency. The "Restricted Role" CIST port setting also mentioned above could also be seen as a security measure.

Point-to-Point

Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Forced True: the port connects to a point-to-point LAN.

Forced False: the port connects to a shared medium.

Auto: the selection of whether the port connects to a point-to-point LAN or to a shared medium is automatically defined. The default is **Auto**.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

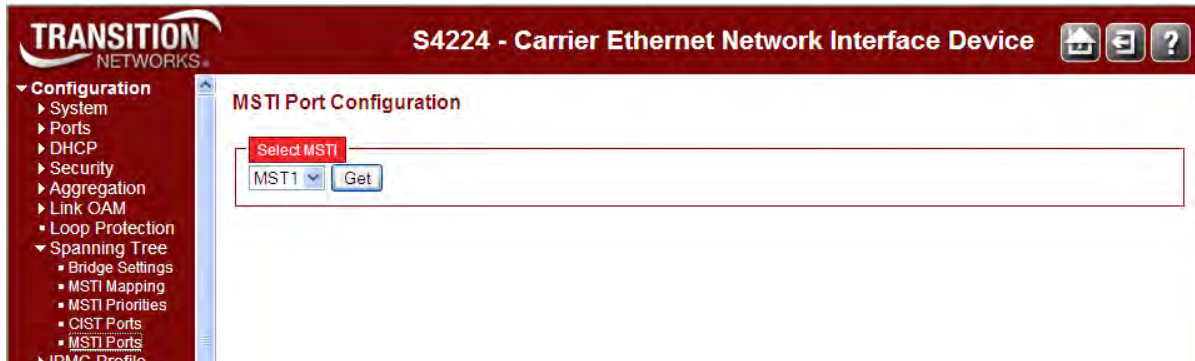
Note:

If you try to enable STP at the **Configuration > Spanning Tree > CST Ports** menu path while the 802.1X **Admin State** is set to any setting other than 'Force Authorized' at **Configuration > Security > Network > NAS**, the message "**STP Error - STP port configuration error**" displays.

You can set the 802.1X **Admin State** to a setting other than 'Force Authorized' at the **Configuration > Security > Network > NAS** menu path. See "[Configuration > Security > Network > NAS](#)" on page 94 for more information.

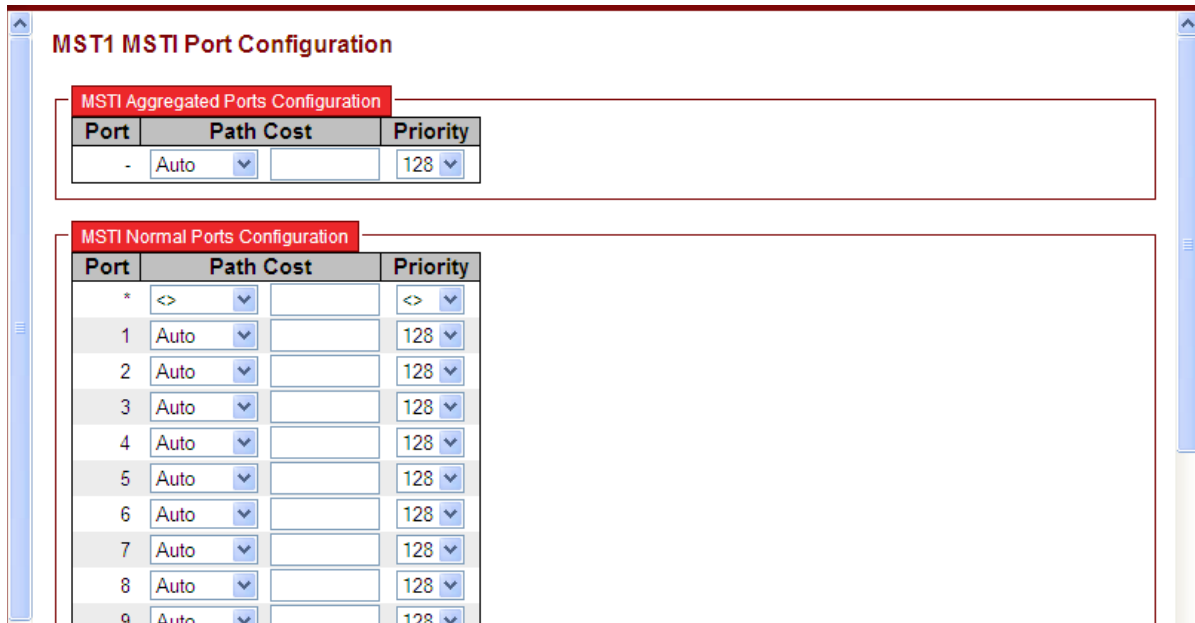
MSTI Ports

MSTI Port Configuration is done from the **Configuration > Spanning Tree > MSTI Ports** menu path.



This page lets you view and/or edit the current STP MSTI port configurations. An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port.

Select the MSTI instance (MST1, MST2, etc.) from the dropdown and click the **Get** button to display the specific MSTI port configuration options:



This page contains MSTI port settings for physical and aggregated ports.

Port

The S4224 port number of the corresponding STP CIST (and MSTI) port.

Path Cost

Controls the path cost incurred by the port.

The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values.

Using the **specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are **1** to **200,000,000**.

Priority

Controls the port priority. This can be used to control the priority of ports having identical port cost. (See above.) At the dropdown, select **0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, or 240**.

The default is **128**.

Buttons

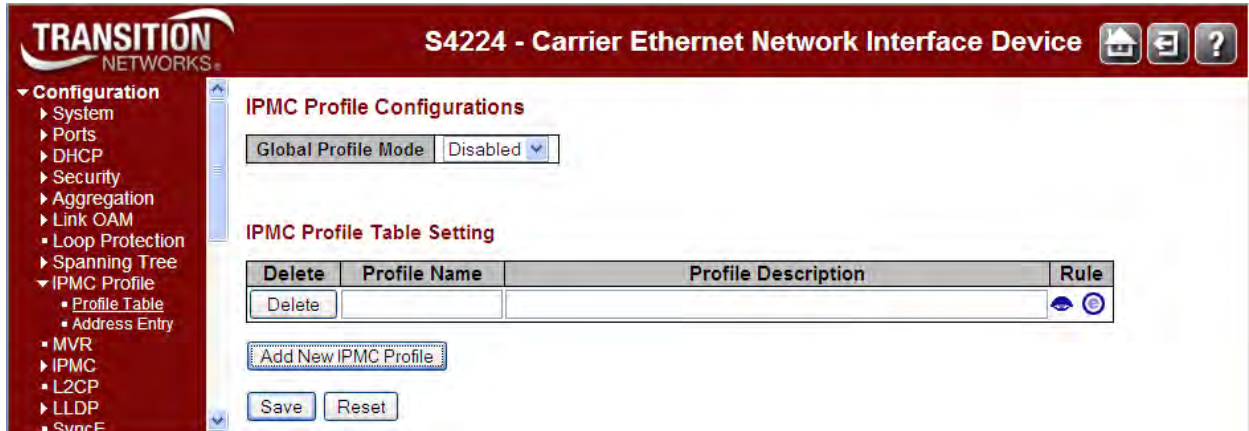
Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

IPMC Profile Configuration

The IPMC profile configuration parameters are available for creating different profiles to deploy the access control on IP Multicast streams. Up to 64 profiles can be created from the **Configuration > IPMC Profile** menu path.

This page provides the filtering rule settings for a specific IPMC profile. It displays the configured rule entries in precedence order. The first rule entry has highest priority in lookup, while the last rule entry has lowest priority in lookup.

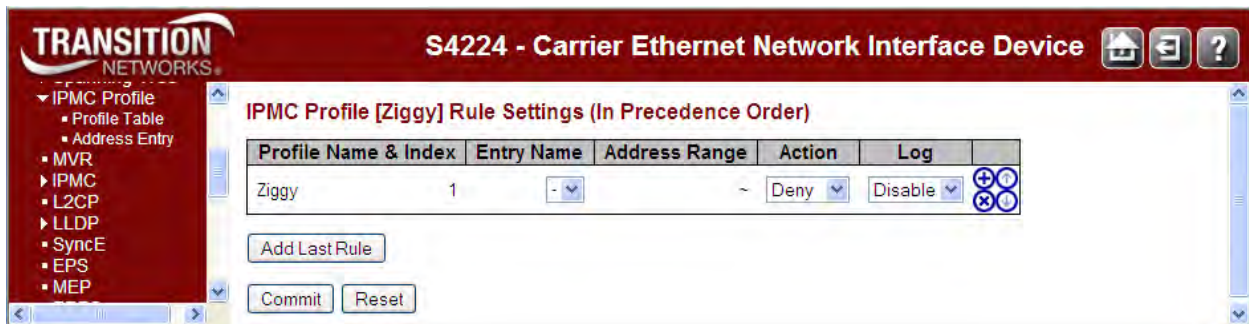


The IP MultiCast profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each.

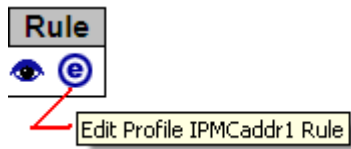
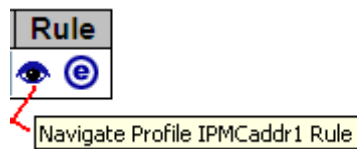
Global Profile Mode

This dropdown lets you Enable/Disable the Global IPMC Profile. When enabled, the S4224 starts to do filtering based on the profile settings only.

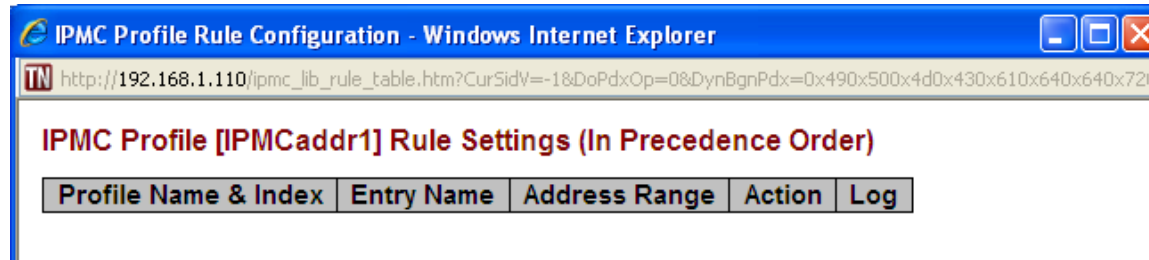
When you click the **Add New IPMC Profile** button the “IPMC Profile [IPMCaddr1]Rule Settings (In Precedence Order)” page displays.



The Rule icons are shown below:



When you add and save a new IPMC profile, click the Navigate icon to display the Profile table shown below:



The Profile table parameters are described below.

> Profile Table

The “IPMC Profile Rule Settings Table” page provides the filtering rule settings for a specific IPMC profile. It displays the configured rule entries in precedence order. First rule entry has highest priority in lookup, while the last rule entry has lowest priority in lookup.

Profile Name

The name of the designated profile to be associated. This field is not editable.

Entry Name

The name used in specifying the address range used for this rule. Only the existing profile address entries will be chosen in the selected box. This field is not allowed to be selected as none ("-") while the Rule Settings Table is committed.

Address Range

The corresponding address range of the selected profile entry. This field is not editable and will be adjusted automatically according to the selected profile entry.

Action

Indicates the learning action upon receiving the Join/Report frame that has the group address matches the address range of the rule.

Permit: Group address matches the range specified in the rule will be learned.

Deny: Group address matches the range specified in the rule will be dropped.

Log





Indicates the logging preference upon receiving the Join/Report frame that has the group address matches the address range of the rule.

Enable: Corresponding information of the group address, that matches the range specified in the rule, will be logged.

Disable: Corresponding information of the group address, that matches the range specified in the rule, will not be logged.

Rule Management Buttons

You can manage rules and the corresponding precedence order by using these buttons:

- : Insert a new rule before the current entry of rule.
- : Delete the current rule entry.
- : Moves the current entry of rule up in the list.
- : Moves the current entry of rule down in the list.

Buttons

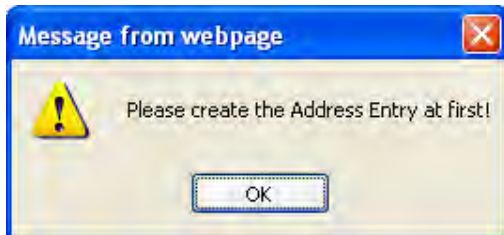
Add Last Rule: Click to add a new rule in the end of the specific profile's rule list. Specify the address entry and configure the new entry. Click "Commit"

Commit: Click to commit rule changes for the designated profile.

Reset: Click to undo any changes made locally and revert to previously saved values.

Messages

Please create the Address Entry first!



Please input valid IPv4/IPv6 multicast start address for Entry xxxxxxx



> Address Entry

The **Configuration > IPMC Profile > Address Entry** menu path displays the “IPMC Profile Address Configuration” page.

When you click the **Add New Address (Range Entry)** button, the editable “IPMC Profile Address Configuration” table displays:

The screenshot shows the web interface for configuring IPMC Profile Address Entries. The page title is "S4224 - Carrier Ethernet Network Interface Device". The main heading is "IPMC Profile Address Configuration". A sidebar on the left shows a navigation menu with "IPMC Profile" expanded to "Address Entry". The main content area includes a "Refresh" button, navigation arrows, and a table with columns "Delete", "Entry Name", "Start Address", and "End Address". Below the table are buttons for "Add New Address (Range) Entry", "Save", and "Reset".

This page provides address range settings used in IPMC profile. The address entry is used to specify the address range that will be associated with IPMC Profile. You can create up to 128 address entries in the system. The parameters are described below.

Delete

Check to delete the entry. The designated entry will be deleted during the next save.

Entry Name

The name used for indexing the address entry table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.

Start Address

The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.

End Address

The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

Buttons

Add New Address (Range) Entry: Click to add new address range. Specify the name and configure the addresses. Click "Save" when done.

Save : Click to save changes.

Reset : Click to undo any changes made locally and revert to previously saved values.

Refresh : Refreshes the displayed table starting from the input fields.

|<< : Updates the table starting from the first entry in the IPMC Profile Address Configuration.

>> : Updates the table, starting with the entry after the last entry currently displayed.

IPMC Profile > Address Entry Example

IPMC Profile [IPTS-3]Rule Settings (In Precedence Order)

| Profile Name & Index | Entry Name | Address Range | Action | Log | |
|----------------------|------------|------------------------|--------|--------|--|
| IPTS-3 1 | IPAC-1 | 224.0.0.0 ~ 224.0.0.10 | Permit | Enable | |

IPMC Profile Configurations

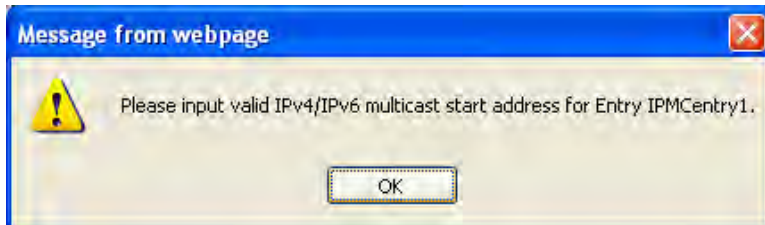
Global Profile Mode:

IPMC Profile Table Setting

| Delete | Profile Name | Profile Description | Rule |
|--------------------------|--------------|---------------------|------|
| <input type="checkbox"/> | IPTS-1 | ProfileOne | |
| <input type="checkbox"/> | IPTS-2 | ProfileTwo | |
| <input type="checkbox"/> | IPTS-3 | ProfileThree | |

Messages

Please input valid IPv4/IPv6 multicast start address for <entry name>



Enter valid starting and ending IPv4/IPv6 Multicast Group Addresses.

See <http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml> for valid address information.

IPMC Parameters Summary

| <u>Configurable Parameter</u> | <u>Allowed Range</u> | <u>Default</u> |
|--------------------------------------|-----------------------------|-----------------------|
| Global Profile Mode | Enabled/Disabled | Disabled |
| Profile name | Up to 16 characters | blank |
| Profile description | Up to 64 characters | blank |

An address entry can be created by specifying a name and a Start and End valid IPv4/IPv6 Multicast address. Up to 128 address entries could be created.

| <u>Configurable Parameter</u> | <u>Allowed Range</u> | <u>Default</u> |
|--------------------------------------|-------------------------------------|-----------------------|
| Entry name | Up to 16 characters | None |
| Start Address | A valid Multicast IPv4/IPv6 address | None |
| End Address | A valid Multicast IPv4/IPv6 address | None |

The following IPMC profile configuration rule settings are available for adding the rules corresponding to an IPMC Profile.

| <u>Configurable Parameter</u> | <u>Allowed Range</u> | <u>Default</u> |
|--------------------------------------|-------------------------------|-----------------------|
| Entry name | A valid Profile address entry | None |
| Action | Deny or Permit | Deny |
| Log | Enabled/Disabled | Disabled |

MVR Configuration

This page provides MVR related configurations from the **Configuration > MVR** menu path. You can view Statistics, MVR Channel Groups, and MVR SFM Information from the **Monitor > MVR** menu path.

Most of the settings are global, whereas the Immediate Leave and MVR Port-Role configuration is related to the current selecting stack unit, as reflected by the page header.

The MVR feature enables multicast traffic forwarding on the Multicast VLANs.

In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

You may create up to four MVR VLANs with a corresponding channel profile for each Multicast VLAN. The channel profile is defined by the IPMC Profile which provides the filtering conditions. Up to four MVR VLANs can be created, and each MVR VLAN manages a channel by using an IPMC profile.

From the default page, click the **Add New MVR VLAN** button to display the edit fields.

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

MVR Mode

Enable or Disable the Global MVR function. The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.

Delete

Check to delete the entry. The designated entry will be deleted during the next save.

MVR VID

Specify the Multicast VLAN ID. **Caution:** MVR source ports are not recommended to be overlapped with management VLAN ports.

MVR Name

MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 16. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.

IGMP Address

Define the IPv4 address as source address used in IP header for IGMP control frames.

The default IGMP address is not set (**0.0.0.0**).

When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.

When the IPv4 management address is not set, system uses the first available IPv4 management address.

Otherwise, system uses a pre-defined value. By default, this value will be **192.0.2.1**.

Mode

Specify the MVR mode of operation. In **Dynamic** mode, MVR allows dynamic MVR membership reports on source ports. In **Compatible** mode, MVR membership reports are forbidden on source ports. The default is **Dynamic** mode.

| Mode |
|------------|
| Dynamic |
| Dynamic |
| Compatible |

Tagging

Specify whether the traversed IGMP/MLD control frames will be sent as **Untagged** or **Tagged** with MVR VID. The default is **Tagged**.

| Tagging |
|----------|
| Tagged |
| Untagged |
| Tagged |

Priority

Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner (**0-7**). The default Priority is **0**.

LLQI

Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a second. The range is from **0 to 31744**. The default LLQI is **5** tenths or one-half second.

Interface Channel Profile

When the MVR VLAN is created, select the IPMC Profile as the channel filtering condition for the specific MVR VLAN. Summary about the Interface Channel Profiling (of the MVR VLAN) will be shown by clicking the view button. The Profile selected for the designated interface channel is not allowed to have overlapped permit group address.

| Interface Channel Profile |
|---------------------------|
| - |
| IPTS-1 |
| IPTS-2 |
| IPTS-3 |

Profile Management Button

You can inspect the rules of the designated profile by using the following button:



: List the rules associated with the designated profile.

Port

The logical port for the settings.

Port Role

Configure an MVR port of the designated MVR VLAN as one of the following roles.

Inactive: The designated port does not participate MVR operations.

Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.

Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.

Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

Select the port role by clicking the Role symbol to switch the setting.

I indicates Inactive; **S** indicates Source; **R** indicates Receiver. The default Role is Inactive.

Immediate Leave

Enable the fast leave on the port. Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

Buttons

Add New MVR VLAN: Click to add new MVR VLAN. Specify the VID and configure the new entry. Edit the parameters as described above. Click **Save** when done.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

IPMC (IP MultiCast)

IP Multicast (IPMC) is a way to send Internet Protocol (IP) datagrams to a group of interested receivers in a single transmission. It is often used for streaming media applications on the Internet and private networks. The method is the IP-specific version of the general concept of multicast networking. It uses specially reserved multicast address blocks in IPv4 and IPv6. In IPv6, IP multicast addressing replaces broadcast addressing as implemented in IPv4. IP multicast is used in enterprises, commercial stock exchanges, and multimedia content delivery networks. One common enterprise use of IP multicast is for IPTV applications such as distance learning and televised company meetings. Multicast is a different transmission mode from unicast, so only protocols designed for multicast are used with multicast.

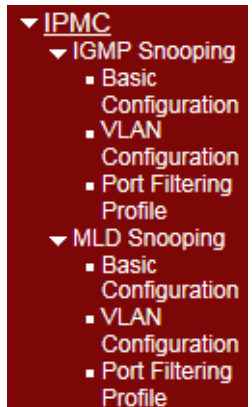
The S4224 IPMC menu provides **IGMP Snooping** and **MLD Snooping** configuration from the **Configuration > IPMC** menu path. These two sub-menus are described in the following sections.

The Internet Group Management Protocol (IGMP) communications protocol is used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP allows more efficient use of resources when supporting online video, gaming, etc.

The S4224 can do IGMPv1/v2/v3 and MLDv1/v2 snooping to limit the broadcast of the IGMP multicast sessions to the ports where the IGMP listeners can be reached. MLD is similar to IGMP except MLD runs over the IPv6 stack. The S4224 looks for IGMP 'join' and 'leave' messages and maintains a table of which ports are part of the conversation. Snooping is enabled at device level and also supports proxying. This feature can be used to avoid forwarding unnecessary join and leave messages to the router interface.

The S4224 also supports IGMP/MLD snooping at VLAN levels. A maximum of 64 VLANs can be chosen for IGMP snooping. Typically the router is the IGMP querier but an option to enable IGMP querier on each VLAN is provided as well on this device. The IGMP querier will send a query in 255 seconds after enabled; if it receives any query from other devices, this will stop querying.

The S4224 provides status on the IGMP sessions and statistics of different queries and messages as discussed later in this section.



IGMP Snooping

The IGMP Snooping menu provides for Basic Configuration, VLAN Configuration, and Port Group Filtering configuration from the sub-menus.

IGMP snooping allows the S4224 dynamically determine which hosts connected to a particular VLAN in the switch need to receive a particular multicast transmission. The S4224 basically listens (snoops) to the various IGMP messages (e.g., 'Query' or 'Leave') and other multicast protocol transmissions. It then dynamically determines which egress ports are associated with each multicast transmission. The S4224 uses a bridge table entry to control multicast forwarding (note that the entry is dynamically configured). The S4224 performs these actions based on IGMP messages snooped: add a receiver to a group, remove a receiver from a group, or maintain group membership.

Basic Configuration

From the **Configuration > IPMC > IGMP Snooping > Basic Configuration** menu path you can view and edit the IGMP Snooping global and port-related configurations.

This page provides IGMP Global and Port Related configuration.

Snooping Enabled

Check to enable Global IGMP Snooping. The default is unchecked (disabled).

Unregistered IPMCv4 Flooding Enabled

Check to enable unregistered IPMC traffic flooding. The default is enabled (checkbox checked). IPMC IP MultiCast (IPMC) supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

IGMP SSM Range

SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. SSM is a method of delivering multicast packets in which the only packets delivered to a receiver are those originating from a specific source address

requested by the receiver. By so limiting the source, SSM reduces demands on the network and improves security. SSM requires that the receiver specify the source address and explicitly excludes the use of the (*,G) join for all multicast groups in [RFC 3376](#), which is possible only in IPv4's IGMPv3 and IPv6's MLDv2.

SSM can be viewed in contrast to ASM (Any-Source Multicast), where a receiver expresses interest in traffic to a multicast address. The multicast network must 1) discover all multicast sources sending to that address, and 2) route data from all sources to all interested receivers. ASM is particularly well suited to groupware applications where 1) all participants in the group want to be aware of all other participants, and 2) the list of participants is not known in advance. With ASM, the source discovery burden on the network can become significant with a large number of sources.

With SSM, the receiver expresses interest in traffic to a multicast address, and also expresses interest in receiving traffic from just one specific source sending to that multicast address. This keeps the network from having to discover numerous multicast sources, and reduces the amount of multicast routing information that the network must maintain. SSM requires support in last-hop routers and in the receiver's operating system. SSM support is not required in other network components (including routers and even the sending host). Interest in multicast traffic from a specific source is conveyed from hosts to routers using IGMPv3 as specified in [RFC 4607](#). In SSM, some types of denial of service (DoS) attack cannot be made by simply sending traffic to a multicast group.

SSM destination addresses must be in the ranges 232.0.0.0/8 for IPv4 or FF3x::/96 for IPv6. See <http://tools.ietf.org/html/rfc4607> for the full set of reserved addresses.

Leave Proxy Enabled

Check to enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side. The default is unchecked.

Proxy Enabled

Check to enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side. The default is unchecked.

Port

The S4224 logical port number. The * in the Port column acts as a 'wild card' character which causes the selections in this row to be applied to all other Ports (rows) in the table for which this selection is valid.

Router Port

Specify which ports act as router ports. A router port is an Ethernet port on the S4224 that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port. The default is unchecked.

Fast Leave

Check to enable the fast leave on the port. With IGMP fast-leave processing enabled, the S4224 immediately removes the interface attached to a receiver on reception of a Leave Group message. This speeds up leave processing, but should only be used when receivers are directly attached to the S4224. The default is unchecked (fast leave disabled on the port).
When you enable IGMP fast-leave processing, the S4224 immediately removes a port when it detects an IGMP v2 leave message on that port.

Throttling

Select **unlimited** or a value from **1 - 10** to limit the number of multicast groups to which an S4224 port can belong. The default is **unlimited**.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

VLAN Configuration

The **Configuration > IPMC > IGMP Snooping > VLAN Configuration** menu path lets you view and edit the IGMP Snooping VLAN Configuration table.

The screenshot shows the web interface for the S4224 - Carrier Ethernet Network Interface Device. The main content area is titled "IGMP Snooping VLAN Configuration". It features a "Refresh" button and navigation arrows. Below the title, there is a "Start from VLAN" input field set to 1 and an "entries per page" input field set to 20. A table displays the configuration for a single VLAN entry:

| Delete | VLAN ID | Snooping Enabled | Querier Election | Querier Address | Compatibility | PRI | RV | QI (sec) | QRI (0.1 sec) | LLQI (0.1 sec) | URI (sec) |
|--------|---------|--------------------------|-------------------------------------|-----------------|---------------|-----|----|----------|---------------|----------------|-----------|
| Delete | | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0.0.0.0 | IGMP-Auto | 0 | 2 | 125 | 100 | 10 | 1 |

Below the table are buttons for "Add New IGMP VLAN", "Save", and "Reset".

Each page shows up to 99 entries from the VLAN table (default of 20) selected through the "entries per page" input field. When first visited, the page shows the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "Start from VLAN" input fields let you select the starting point in the VLAN Table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest VLAN Table match. The **>>** button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached, the text "*No more entries*" displays in the table. Use the **|<<** button to start over.

IGMP Snooping VLAN Table Columns

Delete

Check to delete the entry. The designated entry will be deleted during the next save.

VLAN ID

The VLAN ID (VID) of the entry.

Snooping Enabled

Check to enable the per-VLAN IGMP Snooping. Up to 64 VLANs can be selected. The default is unchecked (per-VLAN IGMP Snooping disabled).

Querier Election

Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Querier Address

Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, the S4224 uses the IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, the S4224 uses the first available IPv4 management address. Otherwise, the S4224 uses a pre-defined value. By default, this value is **192.0.2.1**.

Compatibility

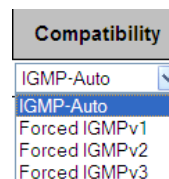
Select **IGMP-Auto**, **Forced IGMPv1**, **Forced IGMPv2**, or **Forced IGMPv3**. Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The default value is **IGMP-Auto**.

IGMP-Auto: Compatibility is automatically assigned (default).

Forced IGMPv1: Compatibility is forced to IGMP version 1.

Forced IGMPv2: Compatibility is forced to IGMP version 2.

Forced IGMPv3: Compatibility is forced to IGMP version 3.



Three versions of IGMP exist - versions v1, v2, and v3. One difference between the versions is how a host node signals that it no longer wants to be a member of a multicast group. In IGMP v1, the host node stops sending reports. If a router does not receive a report from a host node after a predefined length of time (time-out value) it assumes that the host node no longer wants to receive multicast frames and removes it from the membership list of the multicast group. In version 2, a host node exits from a multicast group by sending a leave request. After receiving a leave request from a host node, the router removes the node from appropriate membership list. The router also stops sending multicast packets from the port if it determines there are no further host nodes on the port. Version 3 adds the ability of host nodes to "join" or "leave" specific sources in a multicast group.

PRI

Priority of Interface; indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.

The allowed range is **0** (best effort) to **7** (highest priority). The default interface priority value is **0**.

RV

Displays the Robustness Variable (RV) which allows tuning for the expected packet loss on a network.

The valid range is **1** to **255**. The default robustness variable value is **2**.

QI (sec)

Displays the Query Interval. The Query Interval (QI) is the interval between General Queries sent by the Querier. The valid range is **1** to **255** seconds. The default query interval is **125** seconds.

QRI (0.1 sec)

Displays the Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The valid range is **0** to **31744** in tenths of a second. The default query response interval is **100** in tenths of a second (10 seconds).

LLQI (0.1 sec) (LMQI for IGMP)

Displays the Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The valid range is **0** to **31744** in tenths of a second. The default last member query interval is **10** in tenths of a second (1 second).

URI (sec)

Displays the Unsolicited Report Interval. The Unsolicited Report Interval (URI) is the time between repetitions of a host's initial report of membership in a group. The valid range is **0** to **31744** seconds. The default unsolicited report interval is **1** second.

Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.

|<<: Updates the table starting at the first VLAN Table entry (the entry with the lowest VLAN ID).

>>: Updates the table, starting with the entry after the last entry currently displayed.

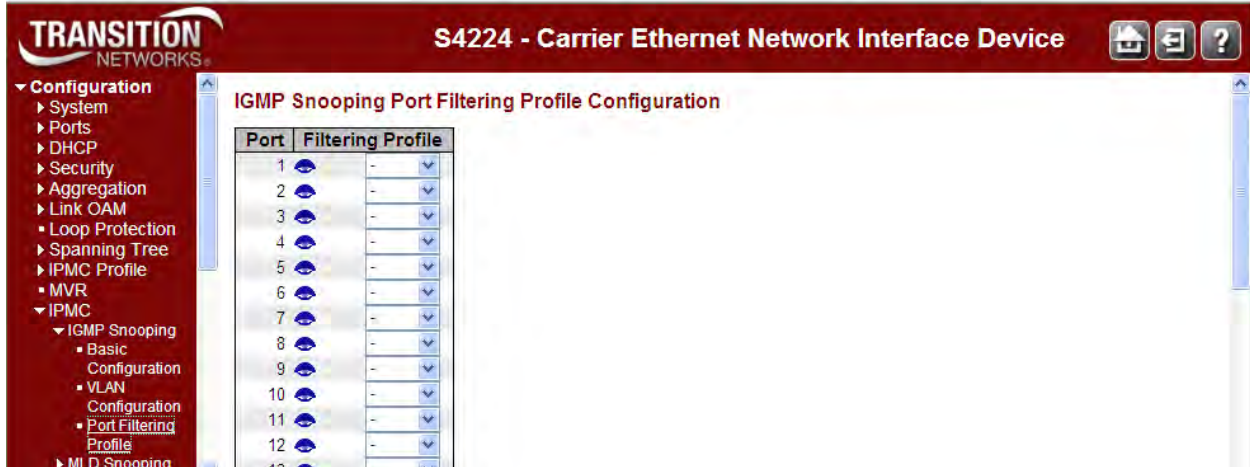
Save: Click to save changes (required to display the

Reset: Click to undo any changes made locally and revert to previously saved values.

Port Filtering Profile

From the **Configuration > IPMC > IGMP Snooping > Port Filtering Profile** menu path you can view and edit the IGMP Snooping Port Filtering Profile Configuration table.

An **IPMC (IP MultiCast) Profile** is used to deploy the access control on IP multicast streams.




Port

The logical port for the settings.

Filtering Profile

Select the IPMC Profile as the filtering condition for the specific port. A summary of the designated profile will be shown by clicking the view button.

Profile Management Button

You can inspect the rules of the designated profile by using the  button to list the rules associated with the designated profile.

IPMC Profile [IPTS-1]Rule Settings (In Precedence Order)

| Profile Name & Index | Entry Name | Address Range | Action | Log |
|----------------------|------------|------------------------|--------|--------|
| IPTS-1 | 1 IPAC-1 | 224.0.0.0 ~ 224.0.0.10 | Permit | Enable |

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Add New Filtering Group: Click to add a new entry to the Group Filtering table.

MLD Snooping

The MLD Snooping menu provides for Basic Configuration, VLAN Configuration, and Port Group Filtering configuration from the sub-menus from the Configuration > IPMC > MLD Snooping menu path..

Multicast Listener Discovery for IPv6 (MLD) is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLD snooping is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. By analyzing received MLD messages, a Layer 2 device running MLD snooping establishes mappings between ports and multicast MAC addresses and forwards IPv6 multicast data based on these mappings. When MLD snooping is not running, IPv6 multicast packets are broadcast to all devices on Layer 2. With MLD snooping running, multicast packets for known IPv6 multicast groups are multicast to the receivers at Layer 2. MLD snooping forwards multicast data to only the receivers requiring it at Layer 2, providing advantages such as reducing Layer 2 broadcast packets for network bandwidth savings, enhancing multicast traffic security, and providing per-host accounting.

Basic Configuration

From the **Configuration > IPMC > MLD Snooping > Basic Configuration** menu path you can view and edit the MLD Snooping global and port configurations.

The screenshot shows the MLD Snooping Configuration page for a S4224 Carrier Ethernet Network Interface Device. The page is divided into two main sections: Global Configuration and Port Related Configuration.

Global Configuration:

- Snooping Enabled:
- Unregistered IPMCv6 Flooding Enabled:
- MLD SSM Range: ff3e:: / 96
- Leave Proxy Enabled:
- Proxy Enabled:

Port Related Configuration:

| Port | Router Port | Fast Leave | Throttling |
|------|--------------------------|--------------------------|------------|
| * | <input type="checkbox"/> | <input type="checkbox"/> | <> |
| 1 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited |
| 4 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited |
| 5 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited |
| 6 | <input type="checkbox"/> | <input type="checkbox"/> | unlimited |

This page provides MLD Snooping related configuration at the global and port level.

Snooping Enabled

Check to enable Global MLD Snooping. The default is unchecked (snooping disabled).

Unregistered IPMC Flooding Enabled

Enable unregistered IPMCv6 traffic flooding. **Note:** disabling unregistered IPMCv6 traffic flooding may cause Neighbor Discovery failure. The default is checked (enabled).

MLD SSM Range

SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers to run the SSM service model for the groups in the address range. SSM destination addresses must be in the ranges 232.0.0.0/8 for IPv4 or FF3x::/96 for IPv6.

SSM Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. SSM is a method of delivering multicast packets in which the only packets delivered to a receiver are those originating from a specific source address requested by the receiver. By so limiting the source, SSM reduces demands on the network and improves security. SSM requires that the receiver specify the source address and explicitly excludes the use of the (*,G) join for all multicast groups in [RFC 3376](#), which is possible only in IPv4's IGMPv3 and IPv6's MLDv2.

SSM is best viewed in contrast to ASM (Any-Source Multicast), where a receiver expresses interest in traffic to a multicast address. The multicast network must 1) discover all multicast sources sending to that address, and 2) route data from all sources to all interested receivers. ASM is particularly well suited to groupware applications where 1) all participants in the group want to be aware of all other participants, and 2) the list of participants is not known in advance. With ASM, the source discovery burden on the network can become significant with a large number of sources.

With SSM, the receiver expresses interest in traffic to a multicast address, and also expresses interest in receiving traffic from just one specific source sending to that multicast address. This keeps the network from having to discover numerous multicast sources, and reduces the amount of multicast routing information that the network must maintain. SSM requires support in last-hop routers and in the receiver's operating system. SSM support is not required in other network components (including routers and even the sending host). Interest in multicast traffic from a specific source is conveyed from hosts to routers using IGMPv3 as specified in [RFC 4607](#). In SSM, some types of denial of service (DoS) attack cannot be made by simply sending traffic to a multicast group.

SSM destination addresses must be in the ranges 232.0.0.0/8 for IPv4 or FF3x::/96 for IPv6. See <http://tools.ietf.org/html/rfc4607> for the full set of reserved addresses.

Leave Proxy Enabled

Check to enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary Leave messages to the router side. The default is unchecked.

Proxy Enabled

Check to enable MLD Proxy. This feature can be used to avoid forwarding unnecessary Join and Leave messages to the router side. The default is unchecked.

Port

The S4224 logical port number. The * in the Port column acts as a 'wild card' character which causes the selections in this row to be applied to all other Ports (rows) in the table for which this selection is valid.

Router Port

Check to specify which ports act as router ports. A router port is a port on the S4224 that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port. The default is unchecked.

Fast Leave

Check to enable the fast leave function on the related port. The default is unchecked. Multicast snooping Fast Leave processing allows the S4224 to remove an interface from the forwarding table entry without first sending out group specific queries to the interface. The VLAN interface is 'pruned' from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. Fast Leave processing applies to both IGMP and MLD. When you enable MLD fast-leave processing, the S4224 immediately removes a port when it detects an IGMP v2 leave message on that port.

Throttling

Used to limit the number of multicast groups to which a S4224 port can belong. Select **unlimited** or **1-10** multicast groups as the limit. The default is **unlimited**.

Buttons

Save: Click to save changes (required to be able to edit all fields).

Reset: Click to undo any changes made locally and revert to previously saved values.

VLAN Configuration

From the **Configuration > IPMC > MLD Snooping > VLAN Configuration** menu path you can view and edit the MLD Snooping VLAN Configuration parameters. Click the **Add New MLD VLAN** button to display the MLD Snooping VLAN Configuration table.

The screenshot displays the 'MLD Snooping VLAN Configuration' page. At the top, it says 'S4224 - Carrier Ethernet Network Interface Device'. The left sidebar shows a navigation tree with 'IPMC' expanded to 'MLD Snooping' > 'VLAN Configuration'. The main content area has a 'Refresh' button and navigation arrows. Below that, it says 'Start from VLAN 1 with 20 entries per page.' A table follows with the following data:

| Delete | VLAN ID | Snooping Enabled | Querier Election | Compatibility | PRI | RV | QI (sec) | QRI (0.1 sec) | LLQI (0.1 sec) | URI (sec) |
|--------------------------|---------|-------------------------------------|------------------|---------------|-----|-----|----------|---------------|----------------|-----------|
| <input type="checkbox"/> | | <input checked="" type="checkbox"/> | MLD-Auto | 0 | 2 | 125 | 100 | 10 | 1 | |

Below the table are buttons for 'Add New MLD VLAN', 'Save', and 'Reset'.

Each page shows up to 99 entries from the VLAN table (default of 20) selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest VLAN Table match. The **>>** button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "*No more entries*" displays in the table. Use the **|<<** button to start over.

The MLD Snooping VLAN table columns are explained below.

Delete

Check to delete the entry. The designated entry will be deleted during the next save.

VLAN ID

The VLAN ID of the entry.

Snooping Enabled

Check to enable the per-VLAN MLD Snooping. Up to 64 VLANs can be selected. The default is unchecked (disabled).

Querier Election

Check to enable the IGMP Querier in the VLAN. The default is unchecked.

Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Querier election is used to dedicate the Querier; only one router sends Query messages, on a particular link. A Querier election rule defines that IGMP Querier or MLD Querier with the lowest IPv4/IPv6 address wins the election.

Compatibility

Select **MLD-Auto**, **Forced MLDv1**, or **Forced MLDv2**. Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The default compatibility value is **MLD-Auto**.

MLD-Auto: Compatibility is automatically assigned.

Forced MLDv1: Compatibility is forced to MLD version 1. MLD v1 was the original release of MLD as an asymmetric protocol, specifying different behaviors for multicast listeners and for routers per IETF [RFC 2710](#).

Forced MLDv2: Compatibility is forced to MLD version 2. MLDv2 is designed to be interoperable with MLDv1. MLDv2 adds the ability for a node to report interest in listening to packets with a particular multicast address only from specific source addresses or from all sources except for specific source addresses. Refer to IETF [RFC 3810](#).

PRI

Priority of Interface indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.

The allowed range is **0** (best effort) to **7** (highest), default interface priority value is **0**.

RV

The Robustness Variable allows tuning for the expected packet loss on a link. The valid range is **1** to **255**, default robustness variable value is **2**.

QI

The Query Interval variable - denotes the interval between General Queries sent by the Querier. The valid range is **1** to **255** seconds. The default query interval is **125** seconds.

QRI (0.1 sec)

Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is **0** to **31744** in tenths of a second. The default query response interval is **100** in tenths of a second (10 seconds).

LLQI (0.1 sec)

The Last Listener Query Interval - the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The valid range is **0** to **31744** in tenths of a second. The default last listener query interval is **10** in tenths of a second (1 second).

URI (sec)

The Unsolicited Report Interval - the time between repetitions of a node's initial report of interest in a multicast address. The valid range is **0** to **31744** seconds. The default URI is **1** second.

Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.

|<<: Updates the table starting from the first entry in the VLAN Table (i.e., the entry with the lowest VLAN ID).

>>: Updates the table, starting with the entry after the last entry currently displayed.

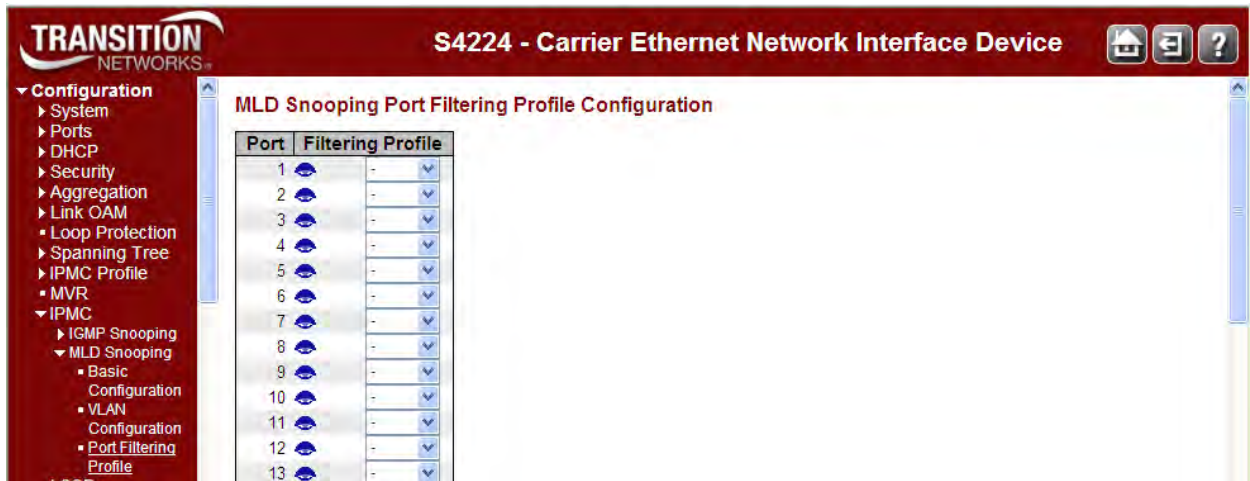
Add New MLD VLAN: Click to add new MLD VLAN. Specify the VID and configure the new entry. Click "Save". The specific MLD VLAN starts working after the corresponding static VLAN is also created.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Port Filtering Profile

From the **Configuration > IPMC > MLD Snooping > Port Filtering Profile** menu path you can view and edit the MLD Snooping Port Filtering Profile parameters.



The Port Filtering Profile table columns are explained below.


Port

The logical port for the settings.

Filtering Profile

Select the IPMC Profile as the filtering condition for the specific port. A summary of the designated profile will be shown by clicking the view button.

Profile Management Button

You can inspect the rules of the designated profile by using the Navigate Profile () buttons to list the rules associated with the designated profile.

IPMC Profile [IPTS-1]Rule Settings (In Precedence Order)

| Profile Name & Index | Entry Name | Address Range | Action | Log |
|----------------------|------------|------------------------|--------|--------|
| IPTS-1 | 1 IPAC-1 | 224.0.0.0 ~ 224.0.0.10 | Permit | Enable |

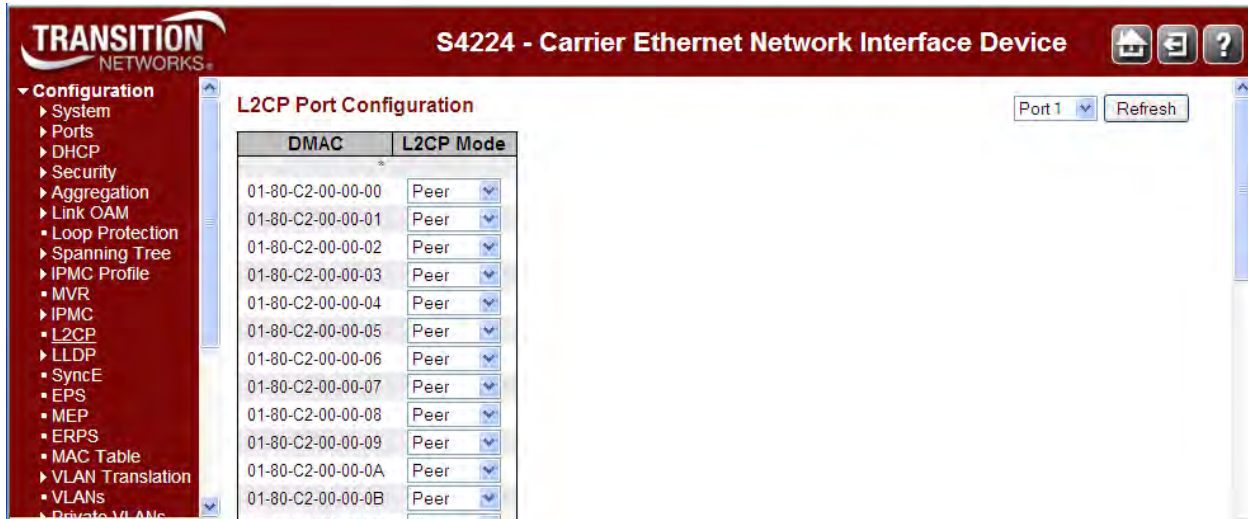
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

L2CP Configuration

This page displays current EVC L2CP configurations and lets you configure the settings. For each service, L2CP protocols are configured to 'peer', 'forward' or 'discard'. Note that while L2CP configuration is performed from the **Configuration > L2CP** menu path, the L2CP command applies not just to Ethernet Services, but to all BPDUs handling.



The L2CP Port Configuration page parameters are described below.

DMAC

The destination BPDUs MAC addresses (01-80-C2-00-00-0X) and GARP (01-80-C2-00-00-2X) MAC addresses for the settings contained in the same row.

L2CP Mode

The L2CP mode for the specific port. The possible values are:

Peer: Redirect to CPU to allow 18 peering/tunneling/discard depending on ECE and protocol configuration.

Forward: Allow to 20 peer/forward/tunnel/discard depending on ECE and protocol configuration.

Discard: Drop frame.

See [MEF 6.1.1](#) for more information. [MEF 45](#) specifies the processing of L2CP Frames for services spanning one or more Carrier Ethernet Networks (CENs).

Buttons

: The port select box determines which port is affected by clicking the buttons.

Refresh: Click to refresh the page.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

LLDP Configuration

The S4224 **Configuration** > **LLDP** menu path lets you configure LLDP at the device level and at the port level. The **Configuration** > **LLDP** menu path also lets you configure LLDP-MED.

LLDP Configuration

From the **Configuration** > **LLDP** menu path you can view and edit the LLDP parameters.

The Link Layer Discovery Protocol (LLDP) IEEE 802.1ab standard protocol allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via LLDP is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP information is sent as an Ethernet frame by devices from each of their interfaces at a fixed interval. Each frame contains one Link Layer Discovery Protocol Data Unit (LLDPDU). Each LLDPDU is a sequence of type-length-value (TLV) structures. The LLDP Ethernet frame typically has its destination MAC address set to a special multicast address that 802.1D-compliant bridges do not forward (other multicast and unicast destination addresses are permitted). The EtherType field is set to 0x88cc. Each LLDP frame starts with mandatory TLVs (Chassis ID, Port ID, and Time-to-Live). The mandatory TLVs are followed by a series of optional TLVs. The frame ends with the 'end of LLDPDU' with both its type and length fields set to 0.

The LLDP Configuration menu is available from the **Configuration** > **LLDP** > **LLDP** menu path.

LLDP Configuration

LLDP Parameters

| | | |
|-------------|----|---------|
| Tx Interval | 30 | seconds |
| Tx Hold | 4 | times |
| Tx Delay | 2 | seconds |
| Tx Reinit | 2 | seconds |

LLDP Interface Configuration

| Interface | Mode | CDP aware | Optional TLVs | | | | |
|---------------------|---------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | | | Port Descr | Sys Name | Sys Descr | Sys Capa | Mgmt Addr |
| GigabitEthernet 1/1 | Enabled | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/2 | Enabled | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/3 | Enabled | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/4 | Enabled | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/5 | Enabled | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/6 | Enabled | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/7 | Enabled | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

This page lets you view and configure the LLDP parameters and port settings as described below.

LLDP Parameters

Tx Interval

The S4224 periodically transmits LLDP frames to its neighbours for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. Valid values are 5 - 32768 seconds. The default is 30 seconds.

Tx Hold

Each LLDP frame contains information about how long the information in the LLDP frame are considered valid. The LLDP information valid period is set to **Tx Hold** multiplied by **Tx Interval** seconds. Valid values are 2 - 10 times. The default is 3 times.

Tx Delay

If some configuration is changed (e.g., the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value. Valid values are 1 - 8192 seconds. The default is 2 seconds.

Tx Reinit

When a port is disabled, LLDP is disabled or the S4224 is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. **Tx Reinit** controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are 1 - 10 seconds. The default is 2 seconds.

LLDP Interface Configuration

Interface

The switch interface name of the logical LLDP interface (e.g., GigabitEthernet 1/1). The * in the Port column acts as a 'wild card' character which causes the selections in this row to be applied to all other Ports (rows) in the table for which this selection is valid.

Mode

Select LLDP mode. The valid selections are:

Disabled The S4224 will not send out LLDP information, and will drop LLDP information received from neighbors.

Enabled The S4224 will send out LLDP information, and will analyze LLDP information received from neighbors.

Rx only The S4224 will not send out LLDP information, but LLDP information from neighbour units is analyzed.

Tx only The S4224 will drop LLDP information received from neighbors, but will send out LLDP information.

CDP aware

Enable or disable CDP (Cisco Discovery Protocol) awareness. The default is disabled (checkbox unchecked). The CDP operation is restricted to decoding incoming CDP frames (the S4224 doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled.

Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbours' table are decoded. All other TLVs are discarded (unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics).

CDP TLVs are mapped onto LLDP neighbours' table as shown below:

CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.

CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbours table.

CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.

CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.

Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbours' table.

If all ports have CDP awareness disabled, then the switch forwards CDP frames received from neighbour devices. If at least one port has CDP awareness enabled, then all CDP frames are terminated by the switch.

Note: When CDP awareness on a port is disabled, the CDP information is not removed immediately, but gets removed when the hold time is exceeded.

Port Descr

Optional TLV: When checked, the "port description" is included in LLDP information transmitted.

An LLDP frame contains multiple TLVs. For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs.

If an optional TLV is disabled, the corresponding information is not included in the LLDP frame.

Sys Name

Optional TLV: When checked, the "system name" is included in LLDP information transmitted.

Sys Descr

Optional TLV: When checked, the "system description" is included in LLDP information transmitted.

Sys Capa

Optional TLV: When checked, the "system capability" is included in LLDP information transmitted.

Mgmt Addr

Optional TLV: When checked, the "management address" is included in LLDP information transmitted.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

The S4224 maintains LLDP port and protocol statistics and a table of neighbors that were discovered. See **Monitor > LLDP** for more information.

LLDP-MED Configuration

From the **Configuration > LLDP > LLDP-MED** menu path you can view and edit the LLDP-MED parameters. LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057). This function applies to VoIP devices which support LLDP-MED.

LLDP-MED Configuration

Fast Start Repeat Count:

Transmit TLVs

| Interface | Capabilities | Priority | Location |
|------------------------|--------------------------|--------------------------|--------------------------|
| 0gigabitEthernet 1/1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/3 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/4 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/5 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/6 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/7 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/8 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/9 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/10 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/11 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/12 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/13 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/14 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/15 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/16 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/17 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/18 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/19 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/20 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/21 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/22 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/23 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0gigabitEthernet 1/24 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 100gigabitEthernet 1/1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 100gigabitEthernet 1/2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 100gigabitEthernet 1/3 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 100gigabitEthernet 1/4 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Coordinates Location

Latitude: North Longitude: East Altitude: Meters Meters Datum: WGS84

Civic Address Location

| Country code | State | County |
|-----------------------|--------------------------|------------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> |
| City | City district | Block (Neighborhood) |
| Street | Leading street direction | Trailing street suffix |
| Street suffix | House no. | House no. suffix |
| Landmark | Additional location info | Name |
| Zip code | Building | Apartment |
| Floor | Room no. | Place type |
| Postal community name | P.O. box | Additional code |

Emergency Call Service

Emergency Call Service:

Policies

Policy ID | Policy ID | Application Type | Tag | VLAN ID | LLDP Priority | Policy

NO. 101-148 (max=8)

Fast Start Repeat Count

Fast start repeat count

Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPDU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count

With this in mind, LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors.

Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With **Fast start repeat count** it is possible to specify the number of

times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

Note that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

Transmit TLVs

It is possible to select which LLDP-MED information that will be transmitted to the neighbors. When the checkbox is checked the information is included in the frame transmitted to the neighbor.

Transmit TLVs

| Interface | Capabilities | Policies | Location |
|---------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| * | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/2 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Interface

The interface name to which the configuration applies (e.g., **GigabitEthernet 1/1**).

Capabilities

When checked the switch's capabilities is included in LLDP-MED information transmitted.

Policies

When checked the configured policies for the interface is included in LLDP-MED information transmitted.

Location

When checked the configured location information for the switch is included in LLDP-MED information transmitted.

Coordinates Location

Latitude

Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either **North** of the equator or **South** of the equator.

Longitude

Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either **East** of the prime meridian or **West** of the prime meridian.

Altitude

Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 1 digits. It is possible to select between two altitude types (floors or meters).

Meters: Representing meters of Altitude defined by the vertical datum specified.

Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

Map Datum

The **Map Datum** is used for the coordinates given in these options:

WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.

NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).

NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). The total number of characters for the combined civic address information must not exceed 250 characters.

Notes on the limitation of 250 characters: 1) A non empty civic address location will use 2 extra characters in addition to the civic address location text. 2) The 2 letter country code is not part of the 250 characters limitation.

Country code

The two-letter ISO 3166 country code in capital ASCII letters (e. g., **DK**, **DE** or **US**).

State

National subdivisions (state, canton, region, province, prefecture).

County

County, parish, gun (Japan), district.

City

City, township, shi (Japan) (e.g., **Copenhagen**).

City district

City division, borough, city district, ward, chou (Japan).

Block (Neighborhood)

Neighborhood, block.

Street

Street (e.g., Poppelvej).

Leading street direction

Leading street direction (e.g., **N** for North).

Trailing street suffix

Trailing street suffix (e.g., **SW** for South West).

Street suffix

Street suffix (e.g., **Platz**).

House no.

House number (e.g., 21).

House no. suffix

House number suffix (e.g., **A**, ½).

Landmark

Landmark or vanity address (e.g., **Columbia University**).

Additional location info

Additional location info (e.g., **South Wing**).

Name

Name (residence and office occupant) (e.g., **Flemming Jahn**).

Zip code

Postal/zip code (e.g., **2791**).

Building

Building (structure) (e.g., **Low Library**).

Apartment

Unit (Apartment, suite) (e.g., **Apt 42**).

Floor

Floor (e.g., **4**).

Room no.

Room number (e.g., **450F**).

Place type

Place type (e.g., **Office**).

Postal community name

Postal community name (e.g., **Leonia**).

P.O. Box

Post office box (P.O. BOX) (e.g., **12345**).

Additional code

Additional code (e.g., **1320300003**).

Emergency Call Service

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Emergency Call Service

Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority value (IEEE 802.1D-2004)
3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control / Signalling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

Note that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

The LLDP-MED Policies are shown and described below:

Policies

| Delete | Policy ID | Application Type | Tag | VLAN ID | L2 Priority | DSCP |
|--------------------------|-----------|------------------|--------|---------|-------------|------|
| <input type="checkbox"/> | 0 | Voice | Tagged | 1 | 0 | 0 |

Delete

Check to delete the policy. It will be deleted during the next save.

Policy ID

ID for the policy. This is auto generated and shall be used when selecting the policies that shall be mapped to the specific ports.

Application Type

Intended use of the application types:

| Application Type |
|-----------------------|
| Voice |
| Voice |
| Voice Signaling |
| Guest Voice |
| Guest Voice Signaling |
| Softphone Voice |
| Video Conferencing |
| Streaming Video |
| Video Signaling |

1. **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. **Voice Signalling** (conditional) - for use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the **Voice** application policy.
3. **Guest Voice** - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
4. **Guest Voice Signalling** (conditional) - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the **Guest Voice** application policy.
5. **Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.
6. **Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. **Streaming Video** - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. **Video Signalling** (conditional) - for use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the **Video Conferencing** application policy.

Tag

Tag indicates whether the specified application type is using a 'tagged' or an 'untagged' VLAN.

Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.

Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

VLAN ID

VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.

L2 Priority

L2 Priority is the Layer 2 priority to be used for the specified application type. **L2 Priority** may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

DSCP

DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. **DSCP** may contain one of 64 code point values (**0 - 63**). A value of **0** represents use of the default DSCP value as defined in IETF RFC 2475.

Adding a New Policy

Click the **Add New Policy** button to add a new policy. Specify the **Application type**, **Tag**, **VLAN ID**, **L2 Priority** and **DSCP** for the new policy. Click "Save". Up to 32 policies are supported.

Policy Interface Configuration

Every interface may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or interface configuration.

Policy Interface Configuration

| Interface | 0 |
|---------------------|--------------------------|
| GigabitEthernet 1/1 | <input type="checkbox"/> |
| GigabitEthernet 1/2 | <input type="checkbox"/> |
| GigabitEthernet 1/3 | <input type="checkbox"/> |

Interface

The interface name to which the configuration applies (e.g., **GigabitEthernet 1/1** or **10GigabitEthernet 1/1**).

Policy Id

The set of policies that shall apply to a given interface. The set of policies is selected by checking the checkboxes that correspond to the policies. A column is created for each Policy that has been configured and saved.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

EPS Configuration

The Ethernet (Linear) Protection Switch (EPS) instances are configured from the **Configuration > EPS** menu path.

Linear Protection is implemented for maintaining connectivity via alternate path in case the current data path fails. Two or more parallel instances are configured between ports of a unit pair. Two of the paths are configured into an Ethernet Protection switching group as a pair of Working-Protecting instances. By default, the designated Working instance is used for data communication. In case of a failure of the Working instance, a Protection switch is executed and the Protecting instance then bears the traffic.

The implementation uses mechanisms defined in Ethernet OAM Specifications (ITU-T.Y.1731) for checking path health. OAM MEPs are configured on instances configured in the Protection Setup between peer units.

Protection Groups can be configured to support revertive or non-revertive mode (i.e., when the Working instance has been restored, whether there should be a Protection switch to use the Working instance again or whether to continue using the Protecting instance).

You can also configure the time to react to instance faults and also to hold for some time between switches, to increase the efficiency of Protection switching and to avoid intermittent or unstable instance conditions.

Different protection schemes (1+1, 1:1, 1:N) can be configured as detailed in the sections below.

Note: Since the protection switching mechanism requires monitoring for both working and protection transport entities, MEPs must be activated for monitoring the working and protection transport entities. See the “[SOAM MEP Configuration](#)” section that follows this section for more information.

When you click the **Add New EPS** button, the Ethernet Protection Switching table display.

The screenshot shows the web interface for the S4224 - Carrier Ethernet Network Interface Device. The main content area is titled "Ethernet Protection Switching" and contains a table with the following columns: Delete, EPS ID, Domain, Architecture, W Flow, P Flow, W SF MEP, P SF MEP, APS MEP, and Alarm. The table has one row with the following values: Delete (Delete button), EPS ID (1), Domain (Port), Architecture (1+1), W Flow (1), P Flow (1), W SF MEP (1), P SF MEP (1), APS MEP (1), and Alarm (empty). Below the table are buttons for "Add New EPS", "Save", and "Reset". A "Refresh" button is located to the right of the table.

The Ethernet (Linear) Protection Switch parameters are explained below.

Delete

This button is used to mark an EPS for deletion in the next Save operation.

EPS ID

The ID of the EPS. Click on the ID of an EPS to enter its configuration page (see below).

Domain

Port: This will create an EPS in the Port Domain. 'W/P Flow' is a Port.

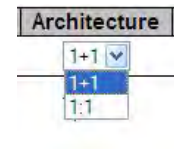
Architecture

Select the linear protection switching architecture; either **1+1** protection switching or **1:1** protection switching architecture.

1+1: This will create a 1+1 EPS. The linear 1+1 protection switching architecture operates with either unidirectional or bidirectional switching. In a 1+1 architecture, a protection transport entity is used to protect the normal traffic signal. At the head-end, the bridge is permanent. Switching occurs only at the tail-end. 1+1 protection is often provisioned as non-revertive operation.

1:1: This will create a 1:1 (bidirectional) EPS. The linear 1:1 protection switching architecture operates with bidirectional switching. In a 1:1 architecture, a protection transport entity is used to protect the normal traffic signal. At the head-end, the bridge is not established until a protection switch is required. 1:1 protection is usually provisioned as revertive operation.

Note: The architecture at each end of the protected domain must match. Bidirectional switching always requires APS communication.



W Flow

Enter the working flow (W Flow) port for the EPS. See the 'Domain' parameter description above.

P Flow

Enter the protecting flow (P Flow) port for the EPS. See the 'Domain' parameter description above.

W SF MEP

Enter the working Signal Fail (SF) reporting MEP.

P SF MEP

Enter the protecting Signal Fail (SF) reporting MEP.

APS MEP

Enter the APS (Automatic Protection Switching) PDU handling MEP.

Alarm

Indicates the alarm status on the EPS. A red dot indicates active alarm and green indicates no active alarms.

Buttons

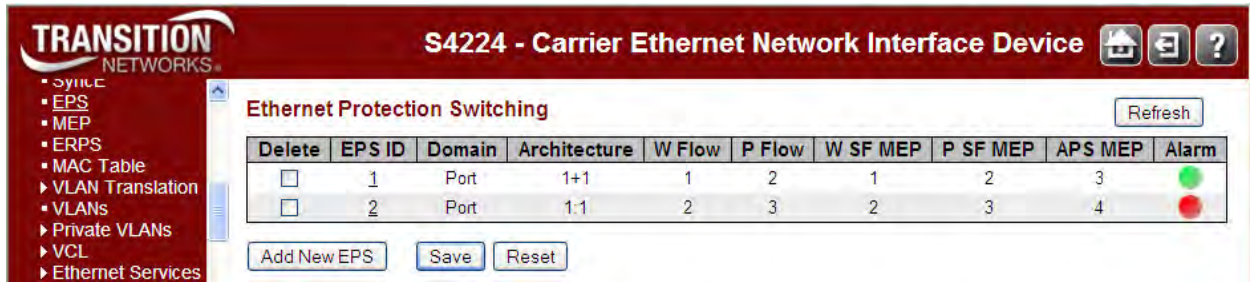
Add New EPS: Click to add a new EPS entry.

Save: Click to save changes.

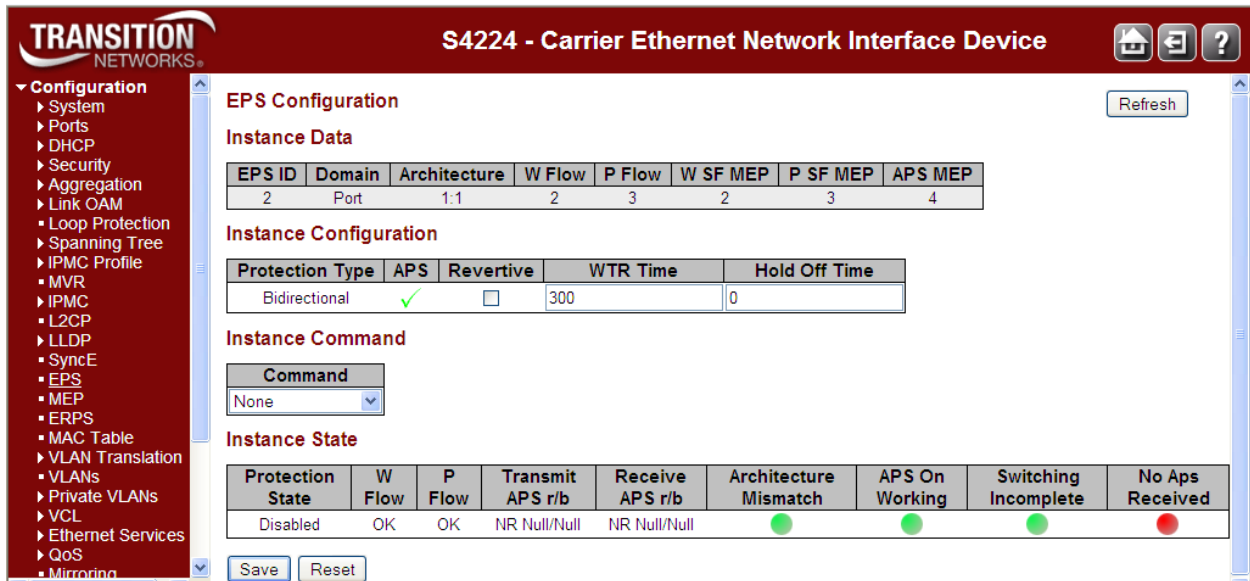
Reset: Click to undo any changes made locally and revert to previously saved values.

EPS Configuration

When you click on the ID of an EPS, its configuration page displays.



For example, if you click on EPS ID 2 on the screen above, the EPS ID 2 configuration screen displays:



This screen lets you configure the EPS Instance Data, Instance Configuration, and Instance Command parameters as well as display the current Instance State.

These parameters are explained below.

EPS Instance Data

This table displays this EPS configuration instance information (EPS ID, Domain, Architecture, W Flow, P Flow, W SF MEP, P SF MEP and APS MEP). See the descriptions above.

EPS Instance Configuration

If configured, the possible Protection Types are:

- 1+1 Unidirectional, no APS communication.
- 1+1 Unidirectional with APS communication.
- 1+1 Bidirectional with APS communication.
- 1:1 Bidirectional with APS communication.

Protection Type

Select Unidirectional or Bidirectional protection mode:

Unidirectional: EPS in the two ends can select traffic from different working/protecting flow. This is only possible in case of 1+1 protection.

Bidirectional: EPS in the two ends is selecting traffic from the same working/protecting flow. This requires APS enabled. This is mandatory for 1:1 protection.

APS

Check or uncheck the checkbox to enable or disable Automatic Protection Switching (the APS protocol). This is mandatory for 1:1 protection. Check the checkbox to enable the automatic protection switching APS protocol and linear protection switching mechanisms for point-to-point VLAN-based ETH SNC (Sub Network Connection) in Ethernet transport networks per Rec. ITU-T G.8031/Y.1342 (11/2009).

Bidirectional switching always requires APS communication. The only switching type that does not require APS communication is 1+1 unidirectional switching.

Revertive

Check or uncheck the checkbox to enable or disable Revertive mode. The revertive switching to working flow can be enabled or disabled here.

Revertive mode: traffic is restored to the working entities after a switch reason has cleared. In the case of clearing a command (e.g., Forced Switch), this happens immediately. In the case of clearing of a defect, this generally happens after the expiry of a “Wait to Restore” timer, which is used to avoid chattering of selectors in the case of intermittent defects.

Operationally, in revertive mode, in conditions where working traffic is being received via the protection entity, if local protection switching requests have been previously active and now become inactive, a local WTR state is entered. Since this state now represents the highest priority local request, it is indicated on the transmitted “Request/State” information and maintains the switch. This state normally times out and becomes a NR state after the WTR timer has expired. The WTR timer is deactivated earlier if any local request of higher priority pre-empts this state.

Note that for the decision of whether or not to enter the WTR state, only local requests are considered. A switch to the protection entity may be maintained by a local WTR state or by a remote request (WTR or other) received via the “Request/State” information. Therefore, in a case where a bidirectional failure for a working entity has occurred and subsequent repair has taken place, the bidirectional reversion back to the working entity does not take place until both WTR timers at both ends have expired.

Non-revertive mode: normal traffic is allowed to remain on the protection entity even after a switch reason has cleared. This is generally accomplished by replacing the previous switch request with a “Do not Revert (DNR)” request, which is low priority.

1+1 protection is often provisioned as non-revertive; the protection is fully dedicated in any case, and this avoids a second “glitch” in the traffic. However there may be reasons to provision this to be revertive (e.g., so that the traffic uses the “short” path except during failure conditions. Certain operator policies also dictate revertive operation even for 1+1).

1:1 protection is usually revertive. It is possible to define the protocol in a way that would permit non-revertive operation for 1:1 protection; however, since the working transport entity is typically more

optimized (i.e., in terms of delay and resourcing) than the protection transport entity, it is better to revert and glitch the traffic when the working transport entity is repaired.

In general, the choice of revertive / non-revertive will be the same at both ends of the protection group. However, a mismatch of this parameter does not prevent interworking; it would be peculiar for one side to go to WTR for clearing of switches initiated from that side, while the other goes to DNR for its switches.

Operationally, in non-revertive mode, in conditions where working traffic is being transmitted via the protection entity, if local protection switching requests have been previously active and now become inactive, a local DNR state is entered. Since this state now represents the highest priority local request, it is indicated on the transmitted "Request/State" information and maintains the switch, thus preventing reversion back to the released bridge/selector position in non revertive mode under NR conditions.

WTR Time

The Wait To Restore timing value to be used in revertive switching. The valid range is 1 - 720 seconds. For example, set the WTR timer to 5 minutes so you are protected by primary line flapping.

In revertive mode, to prevent frequent operation of the protection switch due to an intermittent defect, a failed working transport entity must become fault-free. After the failed working transport entity meets this criterion, a fixed period of time elapses before a normal traffic signal uses it again. This period, called the wait-to-restore (WTR) period, may be configured in 1 minute steps between 5 and 12 minutes; the default value is 5 minutes.

An SF (or SD, if applicable) condition will override the WTR. To activate the WTR timer appropriately even when both ends concurrently detect clearance of SF, when the local state transits from SF to NR with the requested signal number 1, the previous local state, SF, should be memorized. If both the local state and far-end state are NR with the requested signal number 1, the local state transits to WTR only when the previous local state is SF. Otherwise, the local state transits to NR with the requested signal number 0.

In revertive mode, when the protection is no longer requested (i.e., the failed working transport entity is no longer in SF condition - or SD condition, if applicable, and assuming no other requesting transport entities), a local wait-to-restore state is activated. Since this state becomes the highest in priority, it is indicated on the APS signal (if applicable) and maintains the normal traffic signal from the previously failed working transport entity on the protection transport entity. This state normally times out and becomes a no-request state. The WTR timer deactivates earlier when any higher priority request pre-empts this state.

Hold Off Time

The timing value to be used to make persistent check on Signal Fail before switching. This is in 100 ms. and the max value is 100 (10 sec).

You can set the Hold-off timer to 0 so the switchover to backup happens immediately on connection failure.

A hold-off timer is implemented to coordinate the timing of protection switches at multiple layers or across cascaded protected domains. Its purpose is to allow either a server layer protection switch to have a chance to fix the problem before switching at a client layer, or to allow an upstream protected domain to switch before a downstream domain (e.g., to allow an upstream ring to switch before the downstream ring in a dual node interconnect configuration so that the switch occurs in the same ring as the failure).

Each protection group has a configurable hold-off timer. When a new defect or more severe defect occurs (e.g., a new SF), this event will not be reported immediately to protection switching if the provisioned hold-off timer value is non-zero. Instead, the hold-off timer is started; when it expires, it is checked if a defect still exists on the trail that started the timer. If it does, that defect is reported to protection switching. The defect need not be the same one that started the timer. The hold-off timer applies to both the Working and the Protection transport entities.

Command (EPS Instance Command)

At the **Command** dropdown, select None, Clear, Lock Out, Forced Switch, Manual Switch P, Manual Switch W, Exercise, Freeze, or Lock Out Local.

In general MEF terms, a **Manual Switch** occurs when the network operator switches the network to use the protection resources instead of the working, or vice-versa. By MEF definition, a Manual Switch will not progress to failed resources. Manual switch may occur at any time according to the network operator will, unless the target resource is in failure condition. A **Forced Switch** is when the network operator forces the network to use the protection resources instead of the working resources, or vice-versa, regardless of the state of the resources. A **Lockout** command on a resource makes the resource not available for protection of other resources.

The specific S4224 **Command** dropdown selections are explained below.

None: There is no active local command on this instance. This EPS is only created and has not yet been configured - is not active.

Clear: The active local command will be cleared. This EPS is configured - is active. This clears the active near-end lockout of protection, forced switch, manual switch, WTR state, or exercise command. A Clear is an action, initiated externally, that clears the active external command.

Lock Out: This EPS is locked to working (not active). With 1:N protection (more than one EPS with same protecting flow), when one EPS switches to protecting flow, the other EPS enforces this command

Forced Switch: Forced switch to protecting. This forces normal traffic signal to be selected. A Forced switch-over for normal traffic is a switch-over action, initiated externally, that switches normal traffic to the recovery LSP/span, unless an equal or higher priority switch-over command is in effect.

Manual Switch P: Manual switch to protecting. In the absence of a failure of a working or protection transport entity, forces normal traffic signal to be selected. A Manual switch-over for normal traffic is a switch-over action, initiated externally, that switches normal traffic to the recovery LSP/span, unless a fault condition exists on other LSPs/spans (including the recovery LSP/span) or an equal or higher priority switch-over command is in effect.

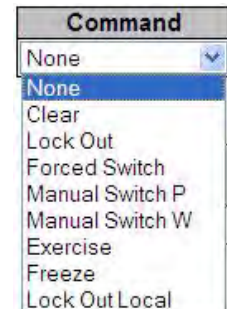
Manual Switch W: Manual switch to working - this is only possible in 1:1 non-revertive.

Exercise: Exercise of the protocol - not traffic effecting. (Exercise of the APS protocol. The signal is chosen so as not to modify the selector.)

Freeze: This EPS is locally frozen, ignoring all input. This freezes the state of the protection group. Until the freeze is cleared, additional near-end commands are rejected. Condition changes and received APS information are ignored. When the freeze command is cleared, the state of the protection group is recomputed based on the condition and received APS information.


A Freeze is a configuration action, initiated externally, that prevents any switch-over action from being taken, and, as such, 'freezes' the current state.

Lock Out Local: This EPS is locally "locked out" - ignoring local SF (signal fail) detected on working.



EPS Instance State

Instance State

| Protection State | W Flow | P Flow | Transmit APS r/b | Receive APS r/b | Architecture Mismatch | APS On Working | Switching Incomplete | No Aps Received |
|------------------|--------|--------|------------------|-----------------|---|---|---|---|
| NoReqW | OK | OK | NR Null/Null | NR Null/Null |  |  |  |  |

Protection State: displays the current EPS state per the State Transition Tables in the G.8031 standard.

Disabled: Protection state currently disabled.

NoReqW: Currently in No request (NR) on working state (lowest priority).

NoReqP: Currently in No request (NR) on protection state (lowest priority).

Lockout: Currently locked out of protection (LO) state. This EPS is locked to the working (not active) state.

Forced: Currently in Forced switch to protecting state.

sfW: Currently in 'Signal Fail on Working' state.

sfP: Currently in 'Signal Fail on Protection' state (SF-P; highest priority).

ManualW: Currently in Manual switch to working (MS-W) state.

ManualP: Currently in Manual switch to protection state.

Wtr: Currently in Wait to Restore (WTR) state.

ExerW: Currently in Exercise (EXER) working state.

ExerP: Currently in Exercise (EXER) protection state.

RevReqW: Currently in Reverse request (RR) working state.

RevReqP: Currently in Reverse request (RR) protection state.

DoNotRev: Currently in Do not revert (DNR) state.

Idle: no detected failure, no active automatic or external command, and receiving only "NR, RB" R-APS messages.

W Flow: Displays Working flow status of **OK**, **SF**, or **SD**, where:

OK: State of working flow is ok

SF: State of working flow is Signal Fail

SD: State of working flow is Signal Degrade (for future use)

P Flow: Displays Protection flow status of **OK**, **SF**, or **SD**, where:

OK: State of protecting flow is ok

SF: State of protecting flow is Signal Fail

SD: State of protecting flow is Signal Degrade (for future use)

Transmit APS r/b: Displays the transmitted APS according to the State Transition Tables in the G.8031 standard. In this field, **RB** indicates '*RPL Blocked*', and **NR** indicates '*No Request*' (e.g., **NR Null/Null** displayed). No request (NR) is the ring protection condition when no local protection switching requests are active. **EXER Null/Normal** indicates Exercise (EXER) protection state null / normal state.

Receive APS r/b: Displays the received APS according to the State Transition Tables in the G.8031 standard. In this field, **rb** indicates '*RPL Blocked*', and **NR** indicates '*No Request*' (e.g., **NR Null/Null** displayed). The status when RPL is blocked (used by RPL Owner in NR).

Architecture Mismatch: Indicates whether the architecture indicated in the received APS does not match the locally configured architecture. Displays a green dot for Up, or a red dot for Down. With all of the options for provisioning, there are opportunities for mismatches between the provisioning at the two ends. These provisioning mismatches take one of several forms, such as Mismatches where proper operation is not possible, or Mismatches where one or both sides can adapt their operation to provide a

degree of interworking in spite of the mismatch, or Mismatches that do not prevent interworking. An example is the revertive / non-revertive mismatch.

APS on working: Indicates whether the APS is received on the working flow. Displays a green dot for Up, or a red dot for Down.

Switching Incomplete: Indicates whether the Traffic is not selected from the same flow instance in the two ends. Displays a green dot for Up, or a red dot for Down.

No APS Received: Indicates if the APS PDU is received from the other end. Displays a green dot for Up, or a red dot for Down.

Note: Since the protection switching mechanism requires monitoring for both working and protection transport entities, MEPs must be activated for monitoring the working and protection transport entities. See the SOAM "[MEP Configuration](#)" section below for more information.

EPS (Port Protection) Parameter Summary

An Ethernet Protection switching Group can be created by configuring these parameters:

| Configurable Parameter | Valid Range | Default |
|--------------------------------|---|----------------|
| EPS Id | 1-100 | 1 |
| Domain | Port / EVC / VLAN | Port |
| Architecture | 1:1/1+1 | 1+1 |
| Working Flow | Valid port range / Flow Id | 1 |
| Protecting Flow | Valid port range / Flow Id | 1 |
| Working SF Reporting MEP | Valid MEP Id | 1 |
| Protecting SF Reporting MEP | Valid MEP Id | 1 |
| APS PDU handling MEP | Valid MEP Id | 1 |
| Instance Configuration | | |
| Protection Type (only for 1+1) | Uni/Bidirectional | Unidirectional |
| APS (only for 1+1) | Enable/Disable | Disabled |
| Revertive | Yes/No | No |
| WTR Time | Disabled / 10sec / 30sec / 5min / 6min / 7min / 8min / 9min / 10min / 11min / 12min | Disabled |
| Hold Off Time | Disabled / 100ms- 900ms (incr 100ms) / 1sec - 10sec (incr1 sec) | Disabled |
| Instance command | None / Clear / LockOut / ForcedSwitch / Manual Switch P / Manual SwitchW / Exercise / Freeze / Lock Out Local | None |

1+1 Port Protection

Two ports on a unit are paired with two ports on a Peer-Unit to create a Working-Protecting pair between the units. After the initialization of Protection Group, Both links are active and transmit data. When a link-failure is detected, the Protecting Link is used to continue data transmission.

1:1 Port Protection

Two ports on a Unit are paired with two ports on a Peer-Unit to create a Working-Protecting pair between the units. After the initialization of Protection Group only the Working Flow is active and both end points of the Protecting Flow are blocked for data transmission. When a link failure is detected on the Working Link, a Protection switch is initiated and the Protecting Link will now be used for active data exchange.

1:N Port Protection

Above sections listed a strict 1:1 redundancy. However, there are two points to consider when setting up redundancy:

- Strict pair redundancy reduces the actual number of usable ports to $n/2$ which may not be the best use of available resources.
- The probability of all or most links failing at the same time is very low.

Considering the above, a 1:N Port Protection scheme is also possible.

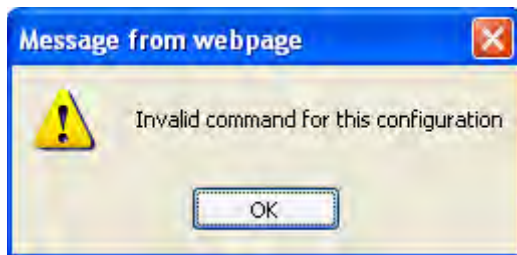
Multiple 1:1 protection groups are configured but the same Protecting Link is chosen in all the groups as a fall-back for the Working Link. Assuming that any of the Working Link fails, a Protection switch to this Protecting Link can be made and traffic can be restored.

Once the faulty Working Link is restored, Automatic (Revertive)/Manual Protection switch can be done to make the Protection Link available to other Groups.

It must be noted that if one of the Working Link is down and a Protection switch is executed, all the other Working Links (with same Protection Link as back-up) go into an administrative hold-mode. This means that if there is a Link Failure in one of these links, there will be no switchover to a Protecting Link.

Messages

Invalid command for this configuration



MEP Configuration

S4224 MEP (Maintenance Entity Group End Point) configuration is done from the **Configuration > MEP** menu path.

A MEP (MEG End Point) is an endpoint in a Maintenance Entity Group (per ITU-T Y.1731).

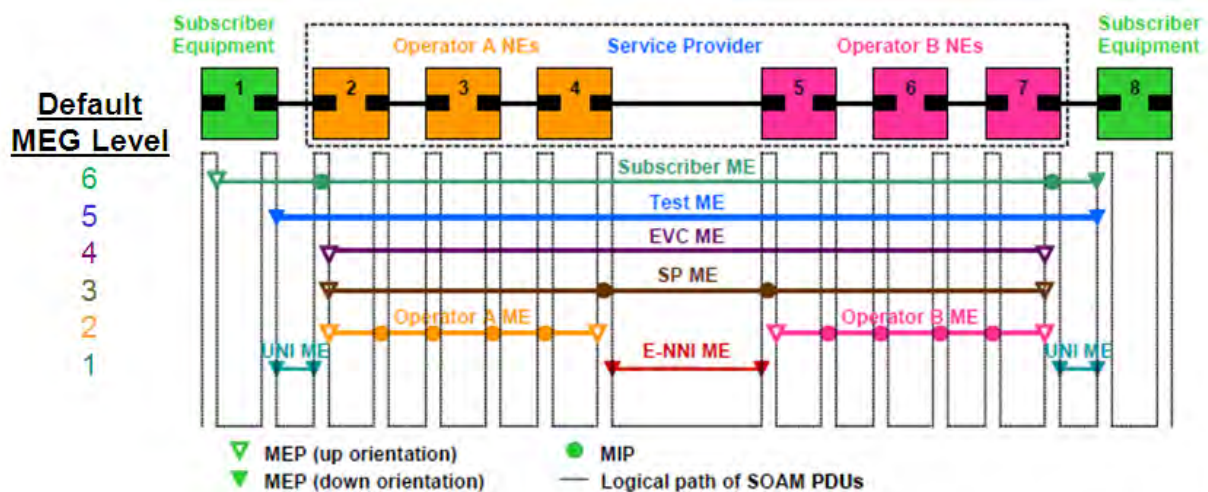
The MEP establishes the path by collating all the LTR PDUs.

A **Down MEP** is a MEP residing in a Bridge that receives SOAM PDUs from, and transmits them towards, the direction of the LAN. Note that in the MEF service model, the LAN is a transmission facility in the egress direction, rather than towards the Bridge Relay Entity. Down MEP

An **Up MEP** is a MEP residing in a Bridge that transmits SOAM PDUs towards, and receives them from, the direction of the Bridge Relay Entity.

A **MIP** (MEG Intermediate Point) is a SOAM point associated with a single MEG level (and a single Maintenance Domain). A MIP can respond to SOAM protocols, but cannot generate requests. MIPs are defined to be located at External Interfaces such as ENNIs (or UNIs). In practice, a MIP can also be used in additional internal operator locations where monitoring is desired.

The default MEG Levels are shown below per MEF 30 (not all MEG levels are required in every application).



The figure above shows pairs of MEPs and MIPs that may communicate across the OAM domains discussed above. The figure also shows the hierarchical relationship between these domains. Note that the orientations of the MEPs in the figure are for example only (not requirements).

Flow OAM is implemented as a set of features as per requirements in IEEE802.1ag and ITU-T.Y1731/G.8021. Nodes can be configured as Maintenance End Point (MEP) or Maintenance Intermediate Point (MIP) in an OAM domain to participate in the Flow OAM functionality. Features such as Link Trace, Continuity Check and Alarm Indication Signal are provided in the implementation.

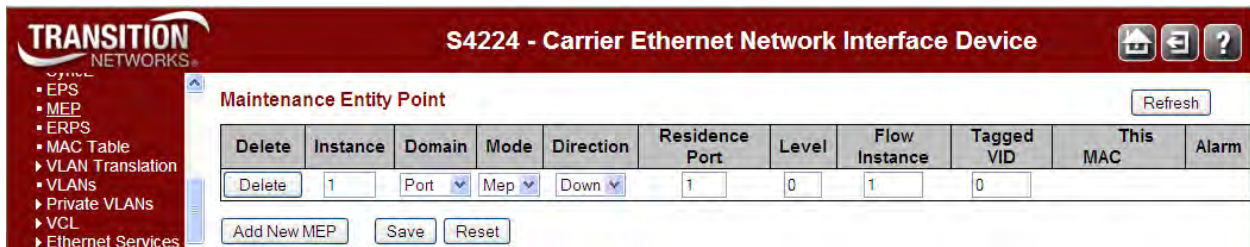
IEEE802.1ag support is implemented with the features like Link Trace, Loopback and Continuity Check. Message parameters are framed as per the IEEE standard when the Link Trace feature configuration indicates IEEE Link Trace. The **LTM** (Link Trace Message) PDU is initiated by MEP. MIPs receive and handle the PDU in a manner that allows the MEP to trace the path to the target MAC address. All intermediate MIPs will forward the packet to the egress port for which the target MAC is learnt and at the same time reply to the MEP with a **LTR** (Link Trace Reply). This continues until the PDU is received by the management point with the target MAC. This entity does not forward the packet but replies to the originator MEP.

ITU-T support is implemented by supporting the following features:

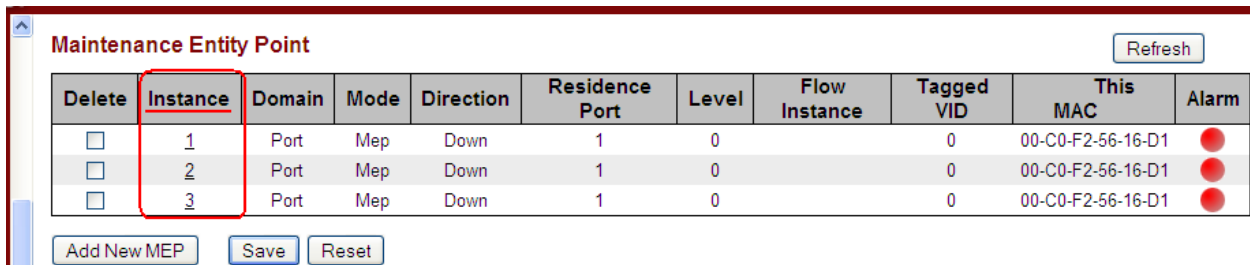
1. Continuity Check – is used for detecting loss of continuity between a MEP and its peer MEP(s). It can also detect unintended connection to other MEG (Maintenance Groups), unintended connection to peer MEP, unexpected period and more.
2. Loop back - is initiated by a MEP to check loop-back path with all peer MEPs in the group.
3. Link Trace - Described in the above section.
4. Alarm Indication Signal (AIS) - is transmitted by a 1 MEP during Signal Fail conditions. It can be used for suppression of alarm on client layer or for protection on client layer
5. Locked Signal - is transmitted by MEP on management demand for administratively locking of a server layer or a sub section of a flow.
6. Loss Measurement - is done between MEPs only. There can only be two MEPs in the group – this is a flow point to point functionality. Both the near-end and the far-end loss can be calculated based of the exchanged information between the MEP. Loss measurement is implemented for CCM based or LMM/LMR based.
7. Delay Measurement - is done between MEP only. There can be many MEPs in the group but DM is done between two MEP only – this is a flow point to multi-point functionality. Both the one-way and the two-way delay + delay variation can be calculated based on the information exchanged between the MEPs. Both One-way and Two-way Delay Measurement is implemented.

Configuration > MEP > Configuration

From the **Configuration > MEP > Configuration** menu path, click the “Add New MEP” button to display the table. The Maintenance Entity Point (MEP) instances are configured here.



When you have configured and saved one or more MEP configurations, you can click on a linked Instance (circled below) to display its MEP Configuration page.



The MEP Configuration page for MEP Instance 1 is shown below.

MEP Configuration Refresh

Instance Data

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|-------------------|
| 1 | Port | Mep | Down | 1 | | 0 | 1 | 00-C0-F2-56-16-D1 |

Instance Configuration

| Level | Format | Domain Name | MEG id | MEP id | Tagged VID | Syslog | cLevel | cMEG | cMEP | cAIS | cLCK | cLoop | cConfig | cSSF | aBLK | aTSF |
|-------|---------|-------------|---------------|--------|------------|--------------------------|--------------------------------------|--------------------------------------|--------------------------------------|--------------------------------------|--------------------------------------|--------------------------------------|--------------------------------------|------------------------------------|--------------------------------------|------------------------------------|
| 0 | ITU ICC | | ICC000MEG0000 | 1 | 0 | <input type="checkbox"/> | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● |

Peer MEP Configuration

| Delete | Peer MEP ID | Unicast Peer MAC | cLOC | cRDI | cPeriod | cPriority |
|-------------------|-------------|------------------|------|------|---------|-----------|
| No Peer MEP Added | | | | | | |

Functional Configuration

| Continuity Check | | | | APS Protocol | | | | |
|--------------------------|----------|------------|--------------------------|--------------------------|----------|-------|-------|------------|
| Enable | Priority | Frame rate | TLV | Enable | Priority | Cast | Type | Last Octet |
| <input type="checkbox"/> | 7 | 1 f/sec | <input type="checkbox"/> | <input type="checkbox"/> | 7 | Multi | L-APS | 1 |

TLV Configuration

| Organization Specific TLV (Global) | | | | |
|------------------------------------|------------|-----------|----------|-------|
| OUI First | OUI Second | OUI Third | Sub-Type | Value |
| 0 | 0 | 12 | 1 | 2 |

TLV Status

| Peer MEP ID | CC Organization Specific | | | | | CC Port Status | | CC Interface Status | | |
|-------------|--------------------------|------------|-----------|----------|-------|----------------|-------|---------------------|-------|---------|
| | OUI First | OUI Second | OUI Third | Sub-Type | Value | Last RX | Value | Last RX | Value | Last RX |
| | | | | | | | | | | |

Link State Tracking

Enable

The MEP parameters are described below.

Delete

This checkbox is used to mark a MEP for deletion in the next Save operation.

Instance

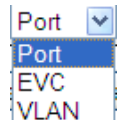
The ID of the MEP. Click on the ID of a MEP to enter the configuration page (see description below).

Domain

Port: This is a MEP in the Port Domain.

Evc: This is a MEP in the EVC Domain. 'Flow Instance' is an EVC. The EVC must exist.

VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In the case of an Up-MEP, the VLAN must already exist.



Mode

Mep: This is a Maintenance Entity End Point.

Mip: This is a Maintenance Entity Intermediate Point. This **MIP** configuration requires **EVC** to be selected in the **Domain** field (above).

Direction

The S4224 MEP direction naming conventions include Down/Ingress and Up/Egress.

Down/Ingress: This is an Ingress/Down MEP - monitoring ingress traffic on the 'Residence Port'.

Up/Egress: This is an Egress/Up MEP - monitoring egress traffic on the 'Residence Port'.

Residence Port

The port where MEP is monitoring - see 'Direction'. For an EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.

Level

The MEG level of this MEP (0-7). The defaults per [MEF 30](#) are:

| MEG | Default MEG Level | Suggested Use (MEF 30) |
|----------------------|--------------------------|---|
| Subscriber MEG | 6 | Subscriber monitoring of an Ethernet service. |
| Test MEG | 5 | SP isolation of subscriber reported problems. |
| EVC MEG | 4 | SP monitoring of provided service. |
| Service Provider MEG | 3 | SP Monitoring of Service Provider network. |
| Operator MEG | 2 | Netw. Operator monitoring of part of a network. |
| UNI MEG | 1 | Service Provider monitoring of a UNI. |
| ENNI MEG | 1 | Network Operators' monitoring of an ENNI. |

(where SP = Service Provider)

Note: Assignment of numerical MEG Levels to 'subscriber' (or customer) role, Service Provider role, and Operator role is somewhat arbitrary since those terms imply business relationships that cannot be standardized. For example, a 'subscriber' (or customer) may also be an Operator seeking a service from another Operator. The MEG Level default values are consistent with a shared MEG Level model across Subscriber, Operators, and Service Providers.

Note: The MEF and Broadband Forum (BBF) are not aligned on the use of MEG Level 5. If interworking between an MEF compliant implementation and a BBF compliant implementation is required, an agreement on the use of MEG Level 5 is required between the two parties.

Flow Instance

The MEP is related to this flow - See 'Domain' above.

Tagged VID

Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID (e.g., 4). A '0' displayed means no Tag to be added with this VID.

Tagged VID

Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.

EVC MEP: This is not used.

VLAN MEP: This is not used.

This MAC

The MAC address (e.g., 00-C0-F2-00-00-02) of this MEP, which can be used by another MEP when unicast is selected (info only). Displays "Not Available" for some domains.

Alarm

There is an active alarm on the MEP. Red LED ● = Down, Green LED ● = Up.

Note: Click the **Refresh** button to verify the status at the end of the configuration process.

Buttons

Add New MEP: Click to add a new MEP entry.

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

MEP Table Parameters

The MEP table parameters are summarized below.

| Parameter | Valid Range | Default |
|----------------|--|---------|
| Instance | 1-100 | 1 |
| Domain | Port, EVC, VLAN | Port |
| Mode | MEP, MIP | MEP |
| Direction | Down, Up | Down |
| Residence Port | 1-number of ports | 1 |
| Level | 0-7 | 0 |
| Flow Instance | 1-128 | 1 |
| Tagged VID | 0-4094 | 0 |
| This MAC | e.g., 00-C0-F2-56-1A-91 or Not Available | -- |
| Alarm | Up = green dot (●) or Down = red dot (●) | -- |

Messages

Warning! The configuration is invalid. EVC flow was found invalid.

Warning! The configuration is invalid. This MIP is not supported.

Warning! The configuration is invalid. VLAN is not created for this VID

Meaning: You tried to set an invalid configuration in the Maintenance Entity Point table at the **Configuration > MEP > Configuration** menu path.

Recovery: 1. Click the **OK** button to clear the message. 2. Change the new MEP config in terms of its Domain, Mode, Direction, etc. 3. Click the **Save** button and continue operation.

MEP Instance Configuration

When you click on the Instance of an MEP in the table, its configuration page displays.

For example, if you click on **2** in the Instance column on the screen above, the MEP Instance 2 configuration screen displays:

Refresh

MEP Configuration

Instance Data

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|-------------------|
| 1 | Port | Mep | Down | 1 | | 0 | 0 | 00-C0-F2-56-1A-91 |

Instance Configuration

| Level | Format | Domain Name | MEG id | MEP id | Tagged VID | VOE | Syslog | cLevel | cMEG | cMEP | cAIS | cLCK | cLoop | cConfig | cSSF | aBLK | aTSF |
|-------|---------|-------------|---------------|--------|------------|--------------------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 0 | ITU ICC | | ICC000MEG0000 | 1 | 0 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Peer MEP Configuration

| Delete | Peer MEP ID | Unicast Peer MAC | cLOC | cRDI | cPeriod | cPriority |
|-------------------|-------------|------------------|------|------|---------|-----------|
| No Peer MEP Added | | | | | | |

Functional Configuration

| Continuity Check | | | | APS Protocol | | | | |
|--------------------------|----------|------------|--------------------------|--------------------------|----------|-------|-------|------------|
| Enable | Priority | Frame rate | TLV | Enable | Priority | Cast | Type | Last Octet |
| <input type="checkbox"/> | 7 | 1 t/sec | <input type="checkbox"/> | <input type="checkbox"/> | 7 | Multi | L-APS | 1 |

TLV Configuration

| Organization Specific TLV (Global) | | | | |
|------------------------------------|------------|-----------|----------|-------|
| OUI First | OUI Second | OUI Third | Sub-Type | Value |
| 0 | 0 | 12 | 1 | 2 |

TLV Status

| Peer MEP ID | CC Organization Specific | | | | | | CC Port Status | | CC Interface Status | |
|-------------|--------------------------|------------|-----------|----------|-------|---------|----------------|---------|---------------------|---------|
| | OUI First | OUI Second | OUI Third | Sub-Type | Value | Last RX | Value | Last RX | Value | Last RX |
| | | | | | | | | | | |

Link State Tracking

Enable

This page lets you configure the MEP Instance Data, Instance Configuration, and Functional Configuration parameters. Here you can add a new peer MEP and configure Fault Management and/or Performance Monitoring.

The parameters are explained below.

MEP Instance Data

Displays this MEP configuration instance information (MEP Instance, Domain, Mode, Direction, Residence Port, Flow Instance, Tagged VID, EPS Instance, and This MAC). See the descriptions above.

Instance Configuration

Level

The MEG level of this MEP (**0-7**).

Format

This is the configuration of the two possible Maintenance Association Identifier formats.

ITU ICC: This is defined by ITU (Y1731 Fig. A3). 'Domain Name' is not used. 'MEG id' must be max. 13 characters.

IEEE String: This is defined by IEEE (802.1ag Section 21.6.5). 'Domain Name' can be max. 16 char. 'MEG id' (Short MA Name) can be max. 16 characters.

ITU CC ICC: This is defined by ITU Y1731 Fig. A5. 'Domain Name' is not used. 'MEG id' must be max. 15 characters.

| Format |
|-------------|
| ITU ICC |
| ITU ICC |
| IEEE String |
| ITU CC ICC |

Domain Name

This is the IEEE Maintenance Domain Name and is only used in case of 'IEEE String' format. This string can be empty giving Maintenance Domain Name Format 1 - Not present. This can be a maximum of 16 characters.

MEG Id

This is either ITU MEG ID or IEEE Short MA Name - depending on 'Format'. See 'Format'. For ITU ICC format this must be 13 characters (e.g., ICC000MEG0000). For ITU CC ICC format this must be 15 characters. For IEEE String format this can be max. 16 characters.

MEP Id

This value will become the transmitted two byte CCM MEP ID.

Tagged VID

This value will be the VID of a TAG added to the OAM PDU.

Syslog

System logging (Syslog) enabled when checked.

Syslog

cLevel

Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP.

cMEG

Fault Cause indicating a CCM is received with a MEG ID different from configured for this MEP.

cMEP

FC indicating CCM received with MEP ID different from all 'Peer MEP ID' configured for this MEP.

cAIS

Fault Cause indicating that AIS PDU is received.

cLCK

Fault Cause indicating that LCK PDU is received.

cLoop

Fault Cause indicating cLoop.

cConfig

Fault Cause indicating cConfig.

cSSF

Fault Cause indicating that server layer is indicating Signal Fail.

aBLK

The consequent action of blocking service frames in this flow is active.

aTSF

The consequent action of indicating Trail Signal Fail towards protection is active.

Peer MEP Configuration**Peer MEP Configuration**

| Delete | Peer MEP ID | Unicast Peer MAC | | cLOC | cRDI | cPeriod | cPriority |
|-------------------|-------------|------------------|--|------|------|---------|-----------|
| No Peer MEP Added | | | | | | | |

Delete

This checkbox is used to mark a Peer MEP for deletion in next Save operation.

Peer MEP ID

This value will become an expected MEP ID in a received CCM - see 'cMEP'. Displays "No Peer MEP Added" by default.

Unicast Peer MAC

This MAC will be used when unicast is selected with this peer MEP. Also, this MAC is used to create hardware checking of receiving CCM PDU (LOC detection) from this MEP.

cLOC

Fault Cause indicating that no CCM has been received (in 3,5 periods) - from this peer MEP.

cRDI

Fault Cause indicating a CCM is received with Remote Defect Indication - from this peer MEP.

cPeriod

Fault Cause indicating a CCM received with a period different configured for this MEP - from this peer MEP.

cPriority

FC indicating a CCM received with different priority than config for this MEP - from this peer MEP.

Buttons

Add New Peer MEP: Click to add and configure a new peer MEP.

Fault Management: Click to go to the Fault Management page.

Performance Monitor: Click to go to the Performance Monitor page.

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

MEP Functional Configuration

Functional Configuration

| Continuity Check | | | | APS Protocol | | | | |
|--------------------------|----------|------------|--------------------------|--------------------------|----------|-------|-------|------------|
| Enable | Priority | Frame rate | TLV | Enable | Priority | Cast | Type | Last Octet |
| <input type="checkbox"/> | 7 | 1 f/sec | <input type="checkbox"/> | <input type="checkbox"/> | 7 | Multi | L-APS | 1 |

Continuity Check

Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. Continuity Check Messages (CCMs) are 'heartbeat' messages exchanged periodically between the MEPs in a service. Each MEP sends out multicast CCMs, and receives CCMs from all the other MEPs in the service (its 'peer' MEPs). This allows each MEP to discover its peer MEPs and to verify that there is connectivity between them. MIPs also receive CCMs; the MIPs use the discovered information to build a MAC learning database for use when responding to a Linktrace.

Enable

Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1.

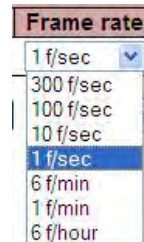
Priority

The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' must be the same.

Frame rate

Select the frame rate of CCM PDU. The selections are 1 f/sec, 300 f/sec, 10 f/sec, 1 f/sec, 6 f/min, 1 f/min, or 6 f/hour. This is the inverse of transmission period as described in Y.1731. This value has the following uses:

- The transmission rate of the CCM PDU.
- Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see 'cLOC'.
- Fault Cause cPeriod is declared if a CCM PDU has been received with a different period - see 'cPeriod'.



Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' must be the same.

TLV

Enable/disable TLV insertion in the CCM PDU.

APS Protocol

APS information is carried within the APS OAM PDU, which is one of a several Ethernet OAM PDUs. OAM PDU formats for each type of Ethernet OAM operation are as defined in Y.1731.

Enable

Automatic Protection Switching protocol information transportation based on transmitting / receiving R-APS/L-APS PDU can be enabled or disabled. This must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured.

Priority

The priority to be inserted as PCP bits in TAG (if any).

Cast

Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. Unicast is only valid for L-APS - see 'Type' below. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032.

Type

R-APS: APS PDU is transmitted as R-APS; this is for ERPS. (Automatic Protection Switching Protocol Data Unit transmitted as Ring APS protocol per Rec. ITU-T G.8032/Y.1344 (03/2010) for Ethernet Ring Protection Switching.)

L-APS: APS PDU is transmitted as L-APS; this is for ELPS (G.8031 Ethernet Linear Protection Switching).

| Type |
|-------|
| L-APS |
| L-APS |
| R-APS |

Last Octet

This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 (03/2010) a RAPS multi-cast MAC is defined as 01-19-A7-00-00-XX. In the current standard, the value for this last octet is '01' and the usage of other values is for further study.

Buttons

Fault Management: Click to go to the Fault Management page (see below).

Performance Monitor: Click to go to the Performance Monitor page (see below).

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Fault Management

Click the **Fault Management** button to view and configure the Fault Management (FM) of the current MEP Instance. Note that after a system reboot, the MEP PM and FM become disabled.

Fault Management - Instance 2

Loop Back

| Enable | DEI | Priority | Cast | Peer MEP | Unicast MAC | To Send | Size | Interval |
|--------------------------|--------------------------|----------|-------|----------|-------------------|---------|------|----------|
| <input type="checkbox"/> | <input type="checkbox"/> | 7 | Multi | 1 | 00-00-00-00-00-00 | 10 | 64 | 100 |

Loop Back State

| Transaction ID | Transmitted | Reply MAC | Received | Out Of Order |
|----------------|-------------|-------------------|----------|--------------|
| 1 | 0 | 00-00-00-00-00-00 | 0 | 0 |

Link Trace

| Enable | Priority | Peer MEP | Unicast MAC | Time To Live |
|--------------------------|----------|----------|-------------------|--------------|
| <input type="checkbox"/> | 7 | 1 | 00-00-00-00-00-00 | 1 |

Link Trace State

| Transaction ID | Time To Live | Mode | Direction | Forwarded | Relay | Last MAC | Next MAC |
|-----------------|--------------|------|-----------|-----------|-------|----------|----------|
| No Transactions | | | | | | | |

Test Signal

| Tx | Rx | DEI | Priority | Peer MEP | Rate | Size | Pattern | Sequence Number |
|--------------------------|--------------------------|--------------------------|----------|----------|------|------|----------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 7 | 1 | 1 | 64 | All Zero | <input type="checkbox"/> |

Test Signal State

| TX frame count | RX frame count | RX rate | Test time | Clear |
|----------------|----------------|---------|-----------|--------------------------|
| 0 | 0 | 0 | 0 | <input type="checkbox"/> |

Client Configuration

| Flow | | | | | | | | | | |
|----------|------|------|------|------|------|------|------|------|------|------|
| Domain | VLAN | VLAN | VLAN | VLAN | VLAN | VLAN | VLAN | VLAN | VLAN | VLAN |
| Instance | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Level | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| AIS prio | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| LCK prio | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

AIS

| Enable | Frame Rate | Protection |
|--------------------------|------------|--------------------------|
| <input type="checkbox"/> | 1 f/sec | <input type="checkbox"/> |

LOCK

| Enable | Frame Rate |
|--------------------------|------------|
| <input type="checkbox"/> | 1 f/sec |

The parameters are described in the following sections.

Loop Back

Enable

Loop Back based on transmitting/receiving LBM/LBR PDU can be enabled or disabled. Loop Back is automatically disabled when all 'To Send' LBM PDUs have been transmitted - waiting 5 seconds for all LBR from the end.

Loopback Messages (LBMs) and Loopback Replies (LBRs) are used to verify connectivity between a local MEP and a particular remote MP. At the request of the administrator, a local MEP sends unicast LBMs to the remote MP. On receiving each LBM, the target maintenance point sends an LBR back to the originating MEP. Loopback indicates whether the destination is reachable or not; it does not allow hop-by-hop discovery of the path; it is conceptually similar to an ICMP Echo (ping).

Dei

The DEI to be inserted as PCP bits in a Tag (if any).

Priority

The priority to be inserted as PCP bits in a Tag (if any).

Cast

Selection of LBM PDU transmitted unicast or multi-cast. The unicast MAC will be configured through 'Peer MEP' or 'Unicast Peer MAC'. Towards MIP only unicast Loop Back is possible. Select 'Uni' or 'Multi'.

Peer MEP

This is only used if the 'Unicast MAC' is configured to all zeros. The LBM unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Unicast MAC

This is only used if NOT configured to all zeros. This will be used as the LBM PDU unicast MAC. This is the only way to configure Loop Back towards a MIP.

To Send

The number of LBM PDU to send in one loop test. The valid range is 1-1000.

Size

The LBM frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing LBM OAM PDU - including CRC (four bytes).

Example: when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + LBM PDU LENGTH(46) + CRC(4) = 64 bytes.

The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC. Minimum Size is 64 Bytes. Maximum Size is 9600 Bytes.

Interval

The interval between transmitting LBM PDU. In 10ms. in case 'To Send' != 0 (max 100 - '0' is as fast as possible) In 1us. in case 'To Send' == 0 (max 10.000)".

Loop Back State

Transaction ID

The transaction id of the first LBM transmitted. For each LBM transmitted (To Send) the transaction id in the PDU is incremented.

Transmitted

The total number of LBM PDU transmitted.

Reply MAC

The MAC of the replying MEP/MIP. In case of multi-cast replies can be received from all peer MEP in the group.

Received

The total number of LBR PDU received from this 'Reply MAC'.

Out Of Order

The number of LBR PDU received from this 'Reply MAC' with incorrect 'Transaction ID'.

Link Trace

Enable

Link Trace based on transmitting/receiving LTM/LTR PDU can be enabled/disabled. Link Trace is automatically disabled when all 5 transactions are done with 5 sec. interval - waiting 5 sec. for all LTR in the end. The LTM PDU is always transmitted as Multi-cast Class 2.

Linktrace Messages (LTMs) and Linktrace Replies (LTRs) are used to track the path, hop-by-hop, to a unicast destination MAC address. At the request of the operator, a local MEP sends an LTM. Each hop that has a maintenance point sends an LTR back to the originating MEP. This allows the administrator to discover connectivity data about the path (conceptually similar to IP traceroute).

Priority

The priority to be inserted as PCP bits in TAG (if any).

Peer MEP

This is only used if the 'Unicast MAC' is configured to all zeros. The Link Trace Target MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Unicast MAC

This is only used if NOT configured to all zeros. This will be used as the Link Trace Target MAC. This is the only way to configure a MIP as Target MAC.

Time To Live

This is the LTM PDU TTL value as described in Y.1731. This value is decremented each time forwarded by a MIP. Will not be forwarded on reaching zero. The valid LT TTL range is 0-255.

Link Trace State

Transaction ID

The transaction ID is incremented for each LTM send. This value is inserted the transmitted LTM PDU and is expected to be received in the LTR PDU. Received LTR with wrong transaction id is ignored. There are five transactions in one Link Trace activated.

Time To Live

This is the TTL value taken from the LTM received by the MIP/MEP sending this LTR - decremented as if forwarded. The valid LT TTL range is 0-255.

Mode

Indicates if it was a MEP/MIP sending this LTR.

Direction

Indicates if MEP/MIP sending this LTR is ingress/egress.

Forwarded

Indicates if MEP/MIP sending this LTR has forwarded the LTM.

Relay

The Relay action can be one of the following:

MAC: The was a hit on the LT Target MAC

FDB: LTM is forwarded based on a hit in the Filtering Database.

MFDB: LTM is forwarded based on hit in the MIP CCM Database.

Last MAC

The MAC identifying the last sender of the LBM causing this LTR - initiating MEP or previous MIP forwarding.

Next Mac

The MAC identifying the next sender of the LBM causing this LTR - MIP forwarding or terminating MEP.

Test Signal

The Ethernet test signal function (ETH-Test) is used to perform one-way on-demand in-service or out-of-service diagnostics tests. This includes verifying bandwidth throughput, frame loss, bit errors, etc. When configured to perform such tests, a MEP inserts frames with ETH-Test information with specified throughput, frame size and transmission patterns. When an out-of-service ETH-Test function is performed, client data traffic is disrupted in the diagnosed entity.

When configured to perform such tests, a MEP inserts frames with ETH-Test information with specified throughput, frame size, and transmission patterns. A test signal generator associated with a MEP can transmit TST frames as often as the test signal generator configuration. When a MEP receives TST frames, it examines them to ensure that the MEG Level corresponds to its own configured MEG Level. If the receiving MEP is configured for the ETH-TST function, the test signal detector associated with the MEP detects bit errors from the pseudo-random bit sequence of the received TST frames and reports such errors.

Enable

Test Signal based on transmitting TST PDU can be enabled or disabled here.

Dei

The DEI to be inserted as PCP bits in Tag (if any).

Priority

The priority to be inserted as PCP bits in Tag (if any).

Peer MEP

This is only used if the 'Unicast MAC' is configured to all zero. The TST frame destination MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Rate

The TST frame transmission bit rate in megabits per second (Mbps). The valid range is 1-400.

Size

The TST frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing TST OAM PDU - including CRC (four bytes).

For example, when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes. The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.

Minimum Size is 64 Bytes. Maximum Size is 9600 Bytes

Pattern

Select **All Zero**, **All One**, or **10101010**. The 'empty' TST PDU has the size of 12 bytes. In order to achieve the configured frame size a data TLV will be added with a pattern.

For example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes.

The TST PDU must be 46 bytes, so a pattern of 46-12=34 bytes will be added.

All Zero: Pattern will be '00000000' (all 0s).

All One: Pattern will be '11111111' (all 1s).

10101010: Pattern will be '10101010' (alternating 1s and 0s).

Test Signal State**Test Signal State**

| TX frame count | RX frame count | RX rate | Test time | Clear |
|----------------|----------------|---------|-----------|--------------------------|
| 0 | 0 | 0 | 0 | <input type="checkbox"/> |

TX frame count

The number of transmitted TST frames since the last 'Clear'. **Note:** The VOE checkbox must be checked under "Instance Configuration" in order for Test Signal TX frame count to display

RX frame count

The number of received TST frames since the last 'Clear'.

RX rate

The current received TST frame bit rate in Kbps. This is calculated on a 1 second basis, starting when first TST frame is received after 'Clear'. The frame size used for this calculation is the first received after 'Clear'.

Test time

The number of seconds passed since first TST frame received after last 'Clear'.

Clear

This will clear all Test Signal State. Transmission of TST frame will be restarted. Calculation of 'Rx frame count', 'RX rate' and 'Test time' will be started when receiving first TST frame.

Client Configuration

Only a Port MEP is able to be a server MEP with flow configuration. The Priority in the client flow is always the highest priority configured in the EVC.

Client Configuration

| Flow | | | | | | | | | | |
|----------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| Domain | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ | VLAN ▾ |
| Instance | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Level | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| AIS prio | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ |
| LCK prio | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ | 0 ▾ |

Domain

The domain of the client layer flow.

VLAN: VLAN domain.

EVC : EVC domain.

Instance

Client layer flow instance numbers.

Level

Client layer level - AIS and LCK PDU transmitted in this client layer flow will be on this level.

AIS prio

The priority to be used when transmitting AIS in each client flow (0-7 and **Highest**). Priority resulting in highest possible PCP can be selected.

LCK prio

The priority to be used when transmitting LCK in each client flow (0-7 and **Highest**). Priority resulting in highest possible PCP can be selected.

Messages

Warning! The configuration is invalid. Invalid COS ID (priority) for this EVC

AIS (Alarm Indication Signal)

Alarm Indication Signal (AIS) messages are used to rapidly notify MEPs when a fault is detected in the middle of a domain, in an event driven way. With AIS, MEPs can learn of a fault much sooner than if they rely on detecting a loss of continuity, etc.

AIS

| Enable | Frame Rate | Protection |
|--------------------------|------------|--------------------------|
| <input type="checkbox"/> | 1 f/sec ▾ | <input type="checkbox"/> |

Enable

Insertion of AIS (AIS PDU transmission) in client layer flows can be enabled or disabled here.

Frame Rate

Select the frame rate of AIS PDU. This is the inverse of transmission period as described in Y.1731.

Select **1f/second** or **1f/minute**.

Protection

Checking this checkbox causes the first three AIS PDUs to be transmitted as fast as possible - in case of using this for protection in the end point.

LOCK

The Ethernet Locked Signal (ETH-LCK) is used to block reaction to a fault situation (much like the ETH-AIS is used to distribute fault conditions). ETH-LCK is normally used in test situations where a change to the network should not result in a protection switch, for example.

LOCK

| Enable | Frame Rate |
|--------------------------|------------|
| <input type="checkbox"/> | 1 f/sec ▾ |

Enable

Insertion of LCK (LCK PDU transmission) in client layer flows can be enable or disabled here.

Frame Rate

Select the frame rate of LCK PDU. This is the inverse of transmission period as described in Y.1731.

Select **1f/second** or **1f/minute**.

Buttons

Back: Return to the “MEP Configuration” page.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page immediately.

Performance Monitoring

Click the **Performance Monitoring** button to view and configure the current MEP Instance Performance Monitoring in terms of LM (Loss Measurement) and DM (Delay measurement). **Note that after a system reboot, the MEP PM and FM become disabled.**

Service provider SLAs depend on the ability to measure and monitor performance metrics for packet loss and one-way and two-way delay, plus related metrics such as delay variation. This measurement ability also provides operators with better visibility into network performance characteristics, thus facilitating planning, troubleshooting, and overall network performance evaluation.

Performance Monitor - Instance 1 Refresh

Performance Monitoring Data Set

Enable

Loss Measurement

| Enable | Priority | Frame rate | Cast | Ended | FLR Interval |
|--------------------------|----------|------------|-------|--------|--------------|
| <input type="checkbox"/> | 7 | 1f/sec | Multi | Single | 5 |

Loss Measurement State

| Tx | Rx | Near End Loss Count | Far End Loss Count | Near End Loss Ratio | Far End Loss Ratio | Clear |
|----|----|---------------------|--------------------|---------------------|--------------------|--------------------------|
| 0 | 0 | 0 | 0 | 0 | 0 | <input type="checkbox"/> |

Delay Measurement

| Enable | Priority | Cast | Peer MEP | Ended | Tx Mode | Calc | Gap | Count | Unit | D2forD1 | Counter Overflow Action |
|--------------------------|----------|-------|----------|--------|-------------|------|-----|-------|------|--------------------------|-------------------------|
| <input type="checkbox"/> | 7 | Multi | 1 | Single | Standardize | Flow | 10 | 10 | us | <input type="checkbox"/> | Keep |

Delay Measurement State

| | Tx | Rx | Rx Timeout | Rx Error | Av Delay Tot | Av Delay last N | Delay Min. | Delay Max. | Av Delay-Var Tot | Av Delay-Var last N | Delay-Var Min. | Delay-Var Max. | Overflow | Clear |
|---------|----|----|------------|----------|--------------|-----------------|------------|------------|------------------|---------------------|----------------|----------------|----------|--------------------------|
| One-way | | | | | | | | | | | | | | |
| F-to-N | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| N-to-F | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Two-way | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input type="checkbox"/> |

Delay Measurement Bins

| Measurement Bins for FD | Measurement Bins for IFDV | Measurement Threshold |
|-------------------------|---------------------------|-----------------------|
| 3 | 3 | 5000 |

Delay Measurement Bins for FD

| | bin0 | bin1 | bin2 |
|---------|------|------|------|
| One-way | | | |
| F-to-N | 0 | 0 | 0 |
| N-to-F | 0 | 0 | 0 |
| Two-way | 0 | 0 | 0 |

Delay Measurement Bins for IFDV

| | bin0 | bin1 | bin2 |
|---------|------|------|------|
| One-way | | | |
| F-to-N | 0 | 0 | 0 |
| N-to-F | 0 | 0 | 0 |
| Two-way | 0 | 0 | 0 |

F-to-N: Far-end-to-near-end
N-to-F: Near-end-to-far-end

Back

Performance Monitoring Data Set

Enable

When enabled this MEP instance will contribute to the 'PM Data Set' gathered by the PM Session.

Loss Measurement

Loss Measurement (LM) offers a way for operators to determine the amount of frame loss in an Ethernet network (e.g., over an EVC). Specifically, LM is the ratio between undelivered OAM frames and the total number of OAM frames transmitted during a specific time interval. ITU-T Y.1731 defines two types of LM:

- 1) Single-Ended, where LM messages are transmitted to another MEP, which includes transmission and reception frame counts in its response message. Here, only the LM initiator is able to derive frame loss from the counters (since it does not include its local counters in the initial LM message); and
- 2) Dual-Ended. Continuity Check messages are used to carry frame transmission and reception counters. In contrast to the single-ended approach, this approach allows all MEPs inside a ME to derive frame loss, instead of only the initiating node.

Loss Measurement

| Enable | Priority | Frame rate | Cast | Ended | FLR Interval | Flow Counting | Oam Counting |
|--------------------------|----------|------------|-------|--------|--------------|--------------------------|--------------|
| <input type="checkbox"/> | 7 | 1 f/sec | Multi | Single | 5 | <input type="checkbox"/> | Y1731 |

Enable

Loss Measurement based on transmitting/receiving CCM or LMM/LMR PDU can be enabled/disabled - see 'Ended'. This is only valid with one Peer MEP configured.

Priority

The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' must be the same for both.

Frame rate

Select the frame rate of CCM/LMM PDU. This is the inverse of transmission period described in Y.1731.

300f/sec selection is not valid.

100f/sec selection is not valid.

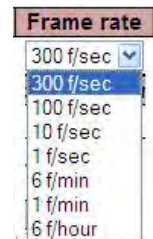
10f/sec selects ten frames-per-second as the frame rate of CCM/LMM PDU.

1f/sec selects one frame-per-second as the frame rate of CCM/LMM PDU.

6f/min selects six frames-per-minute as the frame rate of CCM/LMM PDU.

1f/min selects one frame-per-minute as the frame rate of CCM/LMM PDU.

6f/hour selects six frames-per-hour as the frame rate of CCM/LMM PDU.



If both Continuity Check and Loss Measurement are implemented and enabled on SW based CCM, the 'Frame Rate' must be the same for both.

Cast

Selection of CCM or LMM PDU transmitted **Unicast** or **Multicast**, where:

Uni: The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. If both Continuity Check and dual ended Loss Measurement are implemented and enabled on SW based CCM, the 'Cast' setting must be the same on both.

Multi: CCM or LMM PDU transmitted multicast.

Ended

single: Single-ended Loss Measurement implemented on LMM/LMR.

Dual: Dual-ended Loss Measurement implemented on SW based CCM.

FLR Interval

The interval in seconds where the calculated Frame Loss Ratio (FLR) is displayed (0-65535 seconds).

Flow Counting

Traffic (service frames) are counted per flow - all priority in one.

Oam Counting

Loss Measurement can count OAM frames in different ways.

Y1731: Loss Measurement is counting OAM frames as service frames as described in ITU-T Y1731.

None: Loss Measurement is NOT counting OAM frames as service frames.

All: Loss Measurement is counting all OAM frames as service frames.

Loss Measurement State

Loss Measurement State

| Tx | Rx | Near End Loss Count | Far End Loss Count | Near End Loss Ratio | Far End Loss Ratio | Clear |
|----|----|---------------------|--------------------|---------------------|--------------------|--------------------------|
| 0 | 0 | 0 | 0 | 0 | 0 | <input type="checkbox"/> |

Tx

The transmit count on which the LM is based.

Rx

The receive count on which the LM is based.

Near End Loss Count

The accumulated near end frame loss count - since the last 'Clear'.

Far End Loss Count

The accumulated far end frame loss count - since the last 'Clear'.

Near End Loss Ratio

The near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted - in the latest 'FLR Interval'. The result is given in percent.

Far End Loss Ratio

The far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted - in the latest 'FLR Interval'. The result is given in percent.

Clear

Check this checkbox and Save to clear the accumulated counters and restart ratio calculations.

Delay Measurement

Delay Measurement (DM) can be used for measuring delay in a Carrier Ethernet network. The unit of measurement is the round trip delay of a frame, measured from its first transmitted bit, until the reception of its last bit. Since a DM frame must be sent back to its originating node, LB messages are used.

Frame delay is the difference, in microseconds, between the time an ETH-DM frame is sent and received. (Frame delay variation - the difference between consecutive frame delay values - also called "frame jitter" - is a different parameter.)

Two types of DM can be identified:

One-way measurement: An initiating MEP includes a transmission timestamp in the Ethernet frame. The destination node will capture the frame reception timestamp, and compare both timestamps. As a consequence, the clocks of the sending and receiving nodes need to be synchronized; and

Two-way measurement: In contrast to the one-way measurement, this DM type does not require clock synchronization. The initiating node still includes a timestamp in the Ethernet frame. After the destination node performs a loopback on the frame, the initiating node will receive the frame again. On reception, this node will capture the reception timestamp. Finally, the difference between the timestamps can be calculated.

Delay Measurement

| Enable | Priority | Cast | Peer MEP | Ended | Tx Mode | Calc | Gap | Count | Unit | D2forD1 | Counter Overflow Action |
|--------------------------|----------|-------|----------|--------|-------------|------|-----|-------|------|--------------------------|-------------------------|
| <input type="checkbox"/> | 7 | Multi | 1 | Single | Standardize | Flow | 10 | 10 | us | <input type="checkbox"/> | Keep |

Enable

Delay Measurement based on transmitting 1DM/DMM PDU can be enabled/disabled here. Delay Measurement based on receiving and handling 1DM/DMR PDU is always enabled.

Priority

The priority to be inserted as PCP bits in TAG (if any).

Cast

Selection of 1DM/DMM PDU transmitted **Unicast** or **Multicast**. The unicast MAC will be configured through 'Peer MEP'.

Peer MEP

This is only used if the 'Cast' is configured to 'Uni'. The 1DM/DMR unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer. Frame delay measurement statistics are stored at this MEP for later retrieval.

Ended

single: Single ended Delay Measurement implemented on DMM/DMR.

Dual: Dual ended Delay Measurement implemented on SW based CCM.

| Ended |
|--------|
| Single |
| Single |
| Dual |

Tx Mode

standardize: Transmit 1DM/DMR per the ITU-T Y.1731 standard.

Proprietary: Transmit 1DM/DMR with follow-up packets using a proprietary method.

Calc

This is only used if the 'Way' is configured to Two-way.

Round trip: The frame delay calculated by the transmitting and receiving timestamps of initiators (Frame Delay = RxTimeb-TxTimeStampf).

Flow: The frame delay calculated by the transmitting and receiving timestamps of initiators and remotes. Frame Delay = (RxTimeb-TxTimeStampf)-(TxTimeStampb-RxTimeStampf).

Gap

The gap between transmitting 1DM/DMM PDU in 10 millisecond increments. The valid range is **10** to **65535** milliseconds.

Count

The number of last records to calculate. The range is **10** to **2000** records.

Unit

The time resolution. Select **us** or **ns**.

us: microseconds (uS or μS).

ns: nanoseconds (nS).

D2forD1

Enable to use DMM/DMR packet to calculate one-way DM. If the option is enabled, the following action will be taken. When DMR is received, two-way delay (roundtrip or flow) and both Near-end-to-far-end and Far-end-to-near-end one-way delay are calculated. When DMM or 1DM is received, only Far-end-to-near-end one-way delay is calculated. (Where **D2** indicates two-way delay, and **D1** indicates one-way delay measurement.)

Counter Overflow Action

The action the counter is to take when an overflow occurs.

Keep: Maintain the existing count when an overflow occurs.

Reset: Zero out the counter when an overflow occurs.

Delay Measurement State table

For one-way ETH-DM, only the receiver MEP (on the remote system) collects ETH-DM statistics.

Delay Measurement State

| | Tx | Rx | Rx Timeout | Rx Error | Av Delay Tot | Av Delay last N | Delay Min. | Delay Max. | Av Delay-Var Tot | Av Delay-Var last N | Delay-Var Min. | Delay-Var Max. | Overflow | Clear |
|---------|----|----|------------|----------|--------------|-----------------|------------|------------|------------------|---------------------|----------------|----------------|----------|--------------------------|
| One-way | | | | | | | | | | | | | | |
| F-to-N | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| N-to-F | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Two-way | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input type="checkbox"/> |

F-to-N :Far-end-to-near-end

N-to-F :Near-end-to-far-end

One-way DM performs one-way ETH-DM, which is based on the difference between the time at which the initiator MEP sends a one-way ETH-DM delay measurement request (1DM) frame and the time at which the receiver MEP receives the frame.

F-to-N (Far-end-to-near-end) One-way Delay

The one-way delay is from remote devices to the local devices. The conditions to calculate this delay are:

- 1) 1DM received.
- 2) DMM received with D2forD1 enabled.
- 3) DMR received with D2forD1 enabled.

| | Tx | Rx Timeout | Rx |
|---------|----|------------|----|
| One-way | | | |
| F-to-N | 0 | 0 | 0 |
| N-to-F | 0 | 0 | 0 |
| Two-way | 0 | 0 | 0 |

F-to-N :Far-end-to-near-end

N-to-F :Near-end-to-far-end

N-to-F (Near-end-to-far-end) One-way Delay

The one-way delay is from local devices to remote devices. The only case to calculate this delay is *DMR received with D2forD1 enabled*.

Two-way Delay

Performs two-way ETH-DM, which is based on the difference between the time at which the initiator MEP sends a two-way ETH-DM delay measurement message (DMM) frame and the time at which the initiator MEP receives an associated two-way ETH-DM delay measurement reply (DMR) frame from the responder MEP, subtracting the time elapsed at the responder MEP.

Tx

Displays the accumulated transmit count - since the last 'Clear'.

Rx

The accumulated receive count - since the last 'Clear'.

Rx Timeout

The accumulated receive timeout count for two-way only - since the last 'Clear'.

Av Delay Tot

The average total delay - since last 'clear'.

Av Delay last N

The average delay of the last n packets - since last 'clear'.

Delay Min.

The minimum delay - since last 'clear'.

Delay Max.

The maximum delay - since last 'clear'.

Av Delay-Var Tot

The average total delay variation - since last 'clear'.

Av Delay-Var last N

The average delay variation of the last n packets - since last 'clear'.

Delay-Var Min.

The minimum delay variation - since last 'clear'.

Delay-Var Max.

The maximum delay variation - since last 'clear'.

Overflow

The number of counter overflow - since last 'clear'.

Clear

Set of this checkbox and save will clear the accumulated counters.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Delay Measurement Bins

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

Delay Measurement Bins

| Measurement Bins for FD | Measurement Bins for IFDV | Measurement Threshold |
|-------------------------|---------------------------|-----------------------|
| 3 | 3 | 5000 |

Measurement Bins for FD

Configures the number of Frame Delay Measurement Bins per Measurement Interval.

The minimum number of FD Measurement Bins per Measurement Interval supported is **2**.

The maximum number of FD Measurement Bins per Measurement Interval supported is **10**.

The default number of FD Measurement Bins per Measurement Interval supported is **3**.

Measurement Bins for IFDV

Configures the number of Inter-Frame Delay Variation Measurement Bins per Measurement Interval.

The minimum number of FD Measurement Bins per Measurement Interval supported is **2**.

The maximum number of FD Measurement Bins per Measurement Interval supported is **10**.

The default number of FD Measurement Bins per Measurement Interval supported is **2**.

Measurement Threshold

Configures the Measurement Threshold for each Measurement Bin.

The unit for a measurement threshold is in microseconds (**us**).

The default configured measurement threshold for a Measurement Bin is an increment of **5000 us**.

Delay Measurement Bins for FD

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval. The FD is the Frame Delay per MEF 10.2.

Delay Measurement Bins for FD

| | bin0 | bin1 | bin2 |
|---------|------|------|------|
| One-way | | | |
| F-to-N | 0 | 0 | 0 |
| N-to-F | 0 | 0 | 0 |
| Two-way | 0 | 0 | 0 |

If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

| <u>Bin</u> | <u>Threshold</u> | <u>Range</u> |
|------------|------------------|---------------------------------------|
| bin0 | 0 us | 0 us ≤ measurement < 5,000 us |
| bin1 | 5,000 us | 5,000 us ≤ measurement < 10,000 us |
| bin2 | 10,000 us | 10,000 us ≤ measurement < 15,000 us |
| bin3 | 15,000 us | 15,000 us ≤ measurement < infinite us |

where ≤ means less than or equal to.

Delay Measurement Bins for IFDV

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval. The IFDV is the Inter-Frame Delay Variation per MEF 10.2.

Delay Measurement Bins for IFDV

| | bin0 | bin1 | bin2 |
|---------|------|------|------|
| One-way | | | |
| F-to-N | 0 | 0 | 0 |
| N-to-F | 0 | 0 | 0 |
| Two-way | 0 | 0 | 0 |

F-to-N :Far-end-to-near-end

N-to-F :Near-end-to-far-end

If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

| Bin | Threshold | Range |
|------------|------------------|---------------------------------------|
| bin0 | 0 us | 0 us ≤ measurement < 5,000 us |
| bin1 | 5,000 us | 5,000 us ≤ measurement < 10,000 us |
| bin2 | 10,000 us | 10,000 us ≤ measurement < 15,000 us |
| bin3 | 15,000 us | 15,000 us ≤ measurement < infinite us |

where ≤ means less than or equal to.

TLV Configuration

Configuration of the OAM PDU TLV. Currently only TLV in the CCM is supported.

TLV Configuration

| Organization Specific TLV (Global) | | | | |
|------------------------------------|------------|-----------|----------|-------|
| OUI First | OUI Second | OUI Third | Sub-Type | Value |
| 0 | 0 | 12 | 1 | 2 |

Organization Specific - OUI First

The transmitted first value in the OS TLV OUI field.

Organization Specific - OUI Second

The transmitted second value in the OS TLV OUI field.

Organization Specific - OUI Third

The transmitted third value in the OS TLV OUI field.

Organization Specific - Sub-Type

The transmitted value in the OS TLV Sub-Type field.

Organization Specific - Value

The transmitted value in the OS TLV Value field.

TLV Status

Display of the last received TLV. Currently only TLV in the CCM is supported.

TLV Status

| Peer MEP ID | CC Organization Specific | | | | | | CC Port Status | | CC Interface Status | |
|-------------|--------------------------|------------|-----------|----------|-------|---------|----------------|---------|---------------------|---------|
| | OUI First | OUI Second | OUI Third | Sub-Type | Value | Last RX | Value | Last RX | Value | Last RX |

CC Organization Specific - OUI First

The last received first value in the OUI field.

CC Organization Specific - OUI Second

The last received second value in the OS TLV OUI field.

CC Organization Specific - OUI Third

The last received third value in the OS TLV OUI field.

CC Organization Specific - Sub-Type

The last received value in the OS TLV Sub-Type field.

CC Organization Specific - Value

The last received value in the OS TLV Value field.

CC Organization Specific - Last RX

OS TLV was received in the last received CCM PDU.

CC Port Status - Value

The last received value in the PS TLV Value field.

CC Port Status - Last RX

PS TLV was received in the last received CCM PDU.

CC Interface Status - Value

The last received value in the IS TLV Value field.

CC Interface Status - Last RX

IS TLV was received in the last received CCM PDU.

Link State Tracking**Enable**

When LST is enabled in an instance, Local SF or received 'isDown' in CCM Interface Status TLV, will bring down the residence port. Only valid in Up-MEP.

Link State Tracking

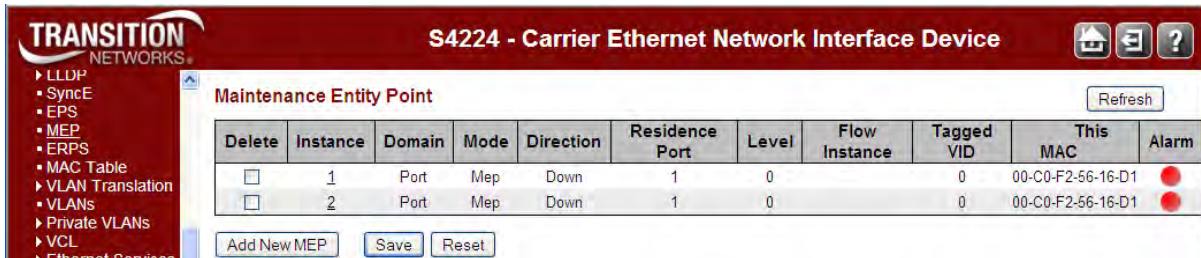
| |
|--------------------------|
| Enable |
| <input type="checkbox"/> |

| | |
|------|-------|
| Save | Reset |
|------|-------|

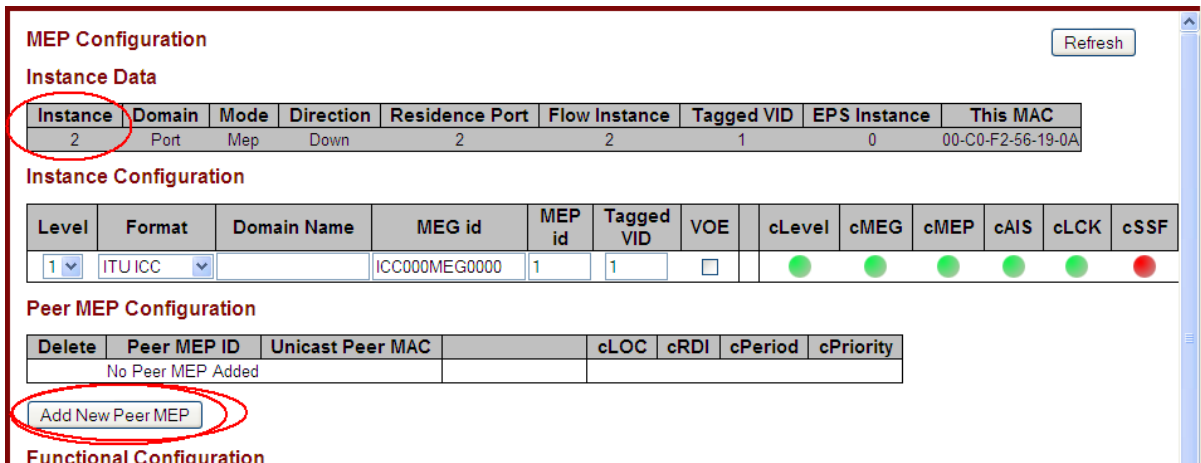
Add a New Peer MEP Procedure

A maximum of 5 Peer MEPs can be added to an instance by clicking the **Add New Peer MEP** button at **Configuration > MEP**. Only one peer MEP can be added per Save operation.

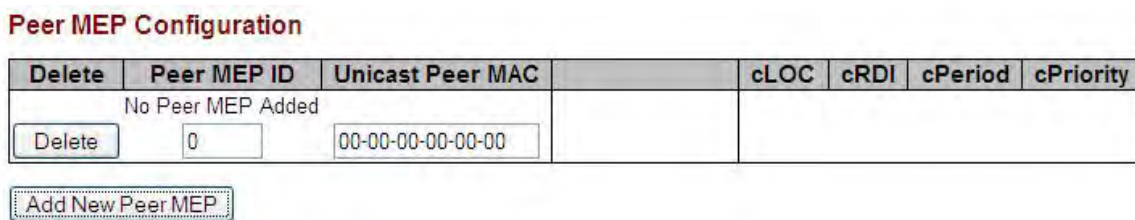
1. Navigate to the **Configuration > MEP** menu path. See “MEP Configuration” on page 213.



2. Select a MEP Instance to configure (e.g., click on the 2 in the **Instance** column above). The MEP Configuration page for MEP Instance 2 displays.



3. In the “Peer MEP Configuration” section, click the **Add New Peer MEP** button. An entry table displays below the message “No Peer MEP Added.”.



4. Enter a unique **Peer MEP ID** for the new peer MEP (you cannot enter duplicate MEP IDs).
5. Enter a **Unicast Peer MAC** address for the new peer MEP (this must be a unicast address).
6. Click the **Save** button.
7. Repeat steps 2-6 for each new peer MEP to be added.

8. Verify your new MEP peer configurations (e.g., Peer MEP IDs 0 and 1 shown below).

MEP Configuration Refresh

Instance Data

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|-------------------|
| 2 | Port | Mep | Down | 2 | 2 | 1 | 0 | 00-C0-F2-56-19-0A |

Instance Configuration

| Level | Format | Domain Name | MEG id | MEP id | Tagged VID | VOE | cLevel | cMEG | cMEP | cAIS | cLCK | cSSF | aBLK | aTSF |
|-------|---------|-------------|---------------|--------|------------|--------------------------|--------------------------------------|--------------------------------------|--------------------------------------|--------------------------------------|--------------------------------------|------------------------------------|--------------------------------------|------------------------------------|
| 1 | ITU ICC | | ICC000MEG0000 | 1 | 1 | <input type="checkbox"/> | ● | ● | ● | ● | ● | ● | ● | ● |

Peer MEP Configuration

| Delete | Peer MEP ID | Unicast Peer MAC | cLOC | cRDI | cPeriod | cPriority |
|--------------------------|-------------|-------------------|--------------------------------------|--------------------------------------|--------------------------------------|--------------------------------------|
| <input type="checkbox"/> | 1 | 22-11-00-00-00-00 | ● | ● | ● | ● |
| <input type="checkbox"/> | 0 | 00-00-00-00-00-00 | ● | ● | ● | ● |

Add New Peer MEP

Functional Configuration

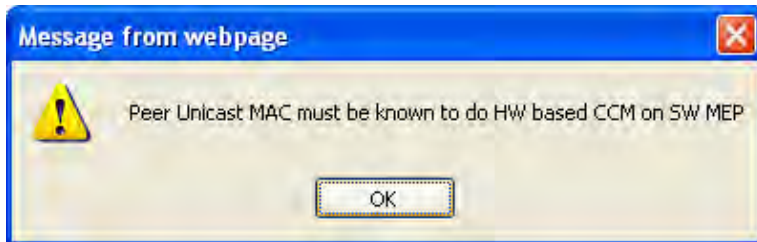
| Continuity Check | | | APS Protocol | | | | |
|--------------------------|----------|------------|--------------------------|----------|-------|-------|------------|
| Enable | Priority | Frame rate | Enable | Priority | Cast | Type | Last Octet |
| <input type="checkbox"/> | 7 | 1f/sec | <input type="checkbox"/> | 7 | Multi | L-APS | 1 |

Fault Management Performance Monitoring

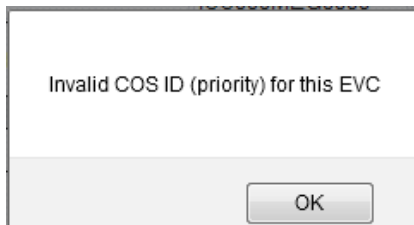
Save Reset

Messages

If the message “Peer Unicast MAC must be known to do HW based CCM on SW MEP” displays, click the **OK** button, then verify that hardware-based CCM is set on the (software) MEP.



If the message “Invalid COS ID (priority) for this EVC” displays, click the **OK** button, then set Actions/Class value and match with CCM Priority.



Delete a Peer MEP Procedure

1. Check an existing Peer MEP's checkbox in the **Delete** column and then click the **Save** button.
2. Verify that the Peer MEP was deleted from the table. Click the Refresh button if necessary.

Add a New MIP Procedure

You can create a MIP on an EVC, but not on a Port. You to select EVC as the Domain and select Up as the Direction, and then select the Level. There is no option to configure a MEG ID, etc.

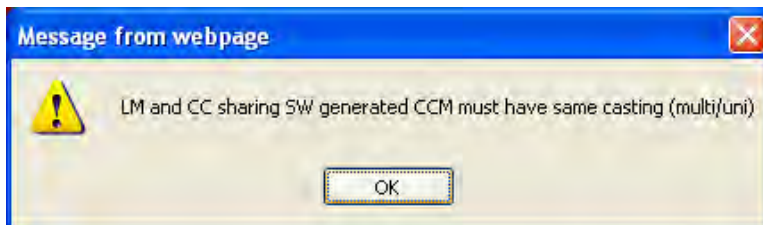
1. Navigate to the **Configuration > Spanning Tree > CIST Ports** menu path and disable STP.
2. Navigate to the **Configuration > VLAN** menu path and configure VLANs as required.
3. Navigate to the **Configuration > MEP** menu path and click the **Add New MEP** button.

| Delete | Instance | Domain | Mode | Direction | Residence Port | Level | Flow Instance | Tagged VID | This MAC | Alarm |
|--------------------------|----------|--------|------|-----------|----------------|-------|---------------|------------|-------------------|------------------------------------|
| <input type="checkbox"/> | 1 | Port | Mep | Down | 1 | 0 | 1 | 0 | 00-C0-F2-56-19-09 | ● |
| <input type="checkbox"/> | 2 | Port | Mep | Down | 2 | 1 | 2 | 1 | 00-C0-F2-56-19-0A | ● |

4. Enter an **Instance** number.
5. At the **Domain** dropdown, select **EVC**.
6. At the **Mode** dropdown, select **MIP**.
7. At the **Direction** dropdown, select **Up**.
8. At the **Residence Port**, **Level**, **Flow Instance**, and **Tagged VID** dropdowns enter valid values (see above).
9. Click the **Save** button when done.

Messages

Message: LM and CC sharing SW generated CCM must have same casting (multi/uni)

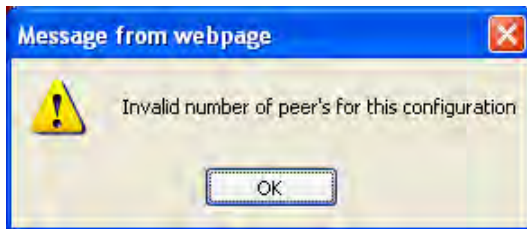


Meaning: You enabled LM or DM in Performance Monitor and Continuity Check or APS Protocol in Fault Management, but both can not be configured at the same time.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Re-configure or disable either Fault Management or Performance Monitoring.

Message: Invalid number of peer's for this configuration.



Meaning: You enabled too many FM functions; only one is allowed at a time.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Re-configure or disable all but one of the Fault Management functions (Loopback, Link Trace, Test Signal, Client Configuration , AIS, and/or LOCK).

MEP Parameter Summary

| Parameter | Valid Range | Default |
|------------------|---------------------------|-------------------|
| Peer MEP ID | 0-8191 | none |
| Unicast Peer MAC | Valid Unicast MAC Address | 00-00-00-00-00-00 |

ERPS Configuration

S4224 ERPS (G.8032 Ethernet Ring Protection Switching) is configured from the **Configuration > ERPS** menu path.

Ethernet Ring Protection is implemented as per the requirements in ITU-T.G.8032 specification. It uses the Continuity Check Message and other OAM frame formats as defined in ITU-T.Y.1731 (specification for Ethernet Operation, Administration and Maintenance-OAM). It is capable of recovering multipoint connectivity in the event of a single ring-link or node failure.

To achieve the objectives of Ring Protection, the ETH layer connectivity of ring links is periodically monitored using CCM. Further the Ring Protection Mechanism communicates with ETH layer and Server layer for Signal Failure notifications to establish link state.

The implementation does not restrict the number of nodes that may form the Ethernet ring. However, from an operational perspective the maximum number of groups is limited to 64.

When you select the **Configuration > ERPS** menu path the default page displays.

At the default Ethernet Ring Protection Switching page, click the **Add New Protection Group** button to display the ERPS table and entry parameters.

The screenshot shows the web interface for S4224 - Carrier Ethernet Network Interface Device. The main heading is "Ethernet Ring Protection Switching". Below the heading is a table with the following columns: Delete, ERPS ID, Port 0, Port 1, Port 0 APS MEP, Port 1 APS MEP, Port 0 SF MEP, Port 1 SF MEP, Ring Type, Interconnected Node, Virtual Channel, Major Ring ID, and Alarm. The table contains one row with the following values: Delete (checkbox checked), ERPS ID (1), Port 0 (1), Port 1 (1), Port 0 APS MEP (1), Port 1 APS MEP (1), Port 0 SF MEP (1), Port 1 SF MEP (1), Ring Type (Major), Interconnected Node (checkbox unchecked), Virtual Channel (checkbox unchecked), Major Ring ID (0), and Alarm (red circle). Below the table are buttons for "Add New Protection Group", "Save", and "Reset".

The ERPS parameters are explained below.

Delete

This checkbox is checked to mark an ERPS for deletion in the next Save operation.

ERPS ID (Protection Group ID)

The ID of the new Protection group. Enter an ID value of 1-64. You can create up to 64 ERPS Protection Groups. You can click on the ID of an existing Protection group to enter its configuration page (described later in this section).

Port 0

This will create a Port 0 of the switch in the ring. Assign an integer value of 1-x. The Port 0 and Port 1 can not be the same.

Port 1

This will create "Port 1" of the switch in the Ring. As the interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. A "0" in this field indicates that no "Port 1" is associated with this instance. Assign an integer value of 1-x. Note that the Port 0 and Port 1 entries can not be the same.

Port 0 APS MEP

This is the Port 0 APS PDU handling MEP. Assign an integer value of **1-x**. The Port 0 APS MEP and Port 1 APS MEP can not be the same. Note that the number refers to the MEP instance number and not the MEP ID (which may or may not be the same).

Port 1 APS MEP

The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance. Assign an integer value of **1-32**. The Port 0 APS MEP and Port 1 APS MEP can not be the same. Note that the number refers to the MEP instance number and not the MEP ID (which may or may not be the same).

Port 0 SF MEP

This is the Port 0 Signal Fail reporting MEP. Assign an integer value of **1-32**. Port 0 SF MEP and Port 1 SF MEP can not be the same. Note that the number refers to the MEP instance number and not the MEP ID (which may or may not be the same).

Port 1 SF MEP

This is the Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. A "0" in this field indicates that no Port 1 SF MEP is associated with this instance. Assign an integer value of **1-32**. Port 0 SF MEP and Port 1 SF MEP can not be the same. Note that the number refers to the MEP instance number and not the MEP ID (which may or may not be the same).

Ring Type

Select the type of Protection ring. It can be either **Major** ring or **Sub-ring**.

Major ring: the Ethernet ring that is connected on two ports to an interconnection node.

Sub-ring: an Ethernet ring which is connected to one or more other Ethernet rings or networks through the use of a pair of interconnection nodes. On their own, the sub-ring links do not form a closed loop. A closed connection of traffic may be formed by the sub-ring links and one or more links that are controlled by other Ethernet ring or network, between interconnection nodes.

Interconnected Node

Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this.

"**Yes**" indicates it is an interconnected node for this instance.

"**No**" indicates that the configured instance is not interconnected.

Virtual Channel

Sub-rings can either have virtual channel or not on the interconnected node. This is configured using this "Virtual Channel" checkbox.

"**Yes**" indicates it is a sub-ring with virtual channel.

"**No**" indicates, sub-ring doesn't have virtual channel. (Sub-ring with or without R-APS virtual channel.)

Sub-ring with R-APS virtual channel: In this option, a virtual channel to tunnel R-APS messages from one interconnection node to the other interconnection node is established.

Sub-ring without R-APS virtual channel: In this option, the R-APS channel is terminated at the interconnection nodes and its R-APS messages are not tunneled between the interconnection nodes. The Ring Interconnection options are shown in Rec. ITU-T G.8032/Y.1344 (03/2010).

R-APS messages are transmitted with the request/state and status information defined by the R-APS request process. The R-APS messages are transported via an R-APS specific VLAN. If the R-APS information to be transmitted has been changed, a burst of three R-APS messages is transmitted as quickly as possible, to ensure the fastest protection switching possible. For messages other than an 'event' message, the R-APS message continues to be transmitted, after the first three messages are

transmitted, with a frequency of one message every five seconds. Typically, R-APS messages are transmitted on both ring ports.

Major Ring ID

This is the Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is Major, this value is same as the protection group ID of this ring.

Alarm

There is an active alarm on the ERPS. A Green dot = Up, a red dot = Down.

Buttons

Add New Protection Group: Click to add and configure a new Protection group entry.

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

When you click on the linked ERPS ID of an existing Protection group, its ERPS Configuration page displays, as discussed below.

ERPS Configuration Page

When you click on the ERPS ID of an existing Protection group, its configuration page displays.

| Delete | ERPS ID | Port 0 | Port 1 | Port 0 APS MEP | Port 1 APS MEP | Port 0 SF MEP | Port 1 SF MEP | Ring Type | Interconnected Node | Virtual Channel | Major Ring ID | Alarm |
|--------------------------|---------|--------|--------|----------------|----------------|---------------|---------------|-----------|---------------------|-----------------|---------------|-------|
| <input type="checkbox"/> | 1 | 2 | 1 | 2 | 1 | 2 | 4 | Major | Yes | No | 1 | ● |
| <input type="checkbox"/> | 2 | 1 | - | 1 | 0 | 1 | 0 | Sub | Yes | No | 0 | ● |
| <input type="checkbox"/> | 3 | 3 | - | 2 | 0 | 3 | 0 | Sub | Yes | No | 0 | ● |
| <input type="checkbox"/> | 4 | 4 | - | 1 | 0 | 1 | 0 | Sub | Yes | No | 0 | ● |

For example, if you click on ERPS ID 2 on the screen above, the ERPS ID 2 configuration displays as shown below:

ERPS Configuration 2Auto-refresh **Instance Data**

| ERPS ID | Port 0 | Port 1 | Port 0 SF MEP | Port 1 SF MEP | Port 0 APS MEP | Port 1 APS MEP | Ring Type |
|---------|--------|--------|---------------|---------------|----------------|----------------|-----------|
| 2 | 1 | 0 | 1 | 0 | 1 | 0 | Sub Ring |

Instance Configuration

| Configured | Guard Time | WTR Time | Hold Off Time | Version | Revertive | VLAN config |
|------------|------------|----------|---------------|---------|-------------------------------------|-----------------------------|
| | 500 | 1min | 0 | v2 | <input checked="" type="checkbox"/> | VLAN Config |

RPL Configuration

| RPL Role | RPL Port | Clear |
|----------|----------|--------------------------|
| None | None | <input type="checkbox"/> |

Sub-Ring Configuration

| Ring Type | Topology Change |
|-----------|--------------------------|
| Sub Ring | <input type="checkbox"/> |

Instance Command

| Command | Port |
|---------|------|
| None | None |

Instance State

| Protection State | Port 0 | Port 1 | Transmit APS | Port 0 Receive APS | Port 1 Receive APS | WTR Remaining | RPL Un-blocked | No APS Received | Port 0 Block Status | Port 1 Block Status | FOP Alarm |
|------------------|--------|--------|--------------|--------------------|--------------------|---------------|----------------|-----------------|---------------------|---------------------|-----------|
| Pending | OK | OK | | | | 0 | | | Blocked | Unblocked | |

This screen lets you configure the ERPS Instance Data, Instance Configuration, RPL Configuration, Sub-Ring Configuration, and Instance Command, and view the ERPS Instance State parameters.

These parameters are explained below.

ERPS Instance Data

ERPS ID

The ID of the new Protection group. Enter an ID value of 1-64. Click on the ID of an existing Protection group to enter its configuration page.

Port 0

This will create a Port 0 of the switch in the ring. Assign an integer value of 1-6. The Port 0 and Port 1 can not be the same.

Port 1

This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance. Assign an integer value of 1-6. The Port 0 and Port 1 can not be the same.

Port 0 SF MEP

This is the Port 0 Signal Fail reporting MEP. Assign an integer value of 1-32. Port 0 SF MEP and Port 1 SF MEP can not be the same. Note that the number refers to the MEP instance number and not the MEP ID (which may or may not be the same).

Port 1 SF MEP

This is the Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. A "0" in this field

indicates that no Port 1 SF MEP is associated with this instance. Assign an integer value of **1-32**. Port 0 SF MEP and Port 1 SF MEP can not be the same. Note that the number refers to the MEP instance number and not the MEP ID (which may or may not be the same).

Port 0 APS MEP

This is the Port 0 APS PDU handling MEP. Assign an integer value of **1-32**. The Port 0 APS MEP and Port 1 APS MEP can not be the same. Note that the number refers to the MEP instance number and not the MEP ID (which may or may not be the same).

Port 1 APS MEP

The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance. Assign an integer value of **1-32**. The Port 0 APS MEP and Port 1 APS MEP can not be the same. Note that the number refers to the MEP instance number and not the MEP ID (which may or may not be the same).

Ring Type

Type of Protection ring. It can be either **Major** ring or **Sub**-ring.

Major ring: the Ethernet ring that is connected on two ports to an interconnection node.

sub-ring: an Ethernet ring which is connected to one or more other Ethernet rings or networks through the use of a pair of interconnection nodes. On their own, the sub-ring links do not form a closed loop. A closed connection of traffic may be formed by the sub-ring links and one or more links, that are controlled by other Ethernet ring(s) or network(s), between interconnection nodes.

ERPS Instance Configuration

Configured

Displays a green LED (●) for Up or a red LED (●) for Down.

Red: This ERPS is only created and has not yet been configured and is not active.

Green: This ERPS is configured and is active.

Guard Time

Enter the Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. The period of the guard timer can be configured in 10 ms steps between **10 ms** and **2 seconds**, with a default value of **500 ms**. The guard timer is used to prevent Ethernet ring nodes from acting on outdated R-APS messages, and prevents the possibility of forming a closed loop. The guard timer is activated whenever an Ethernet ring node receives an indication that a local switching request has cleared (i.e., Local Clear SF, Clear). This guard timer period should be greater than the maximum expected forwarding delay in which an R-APS message traverses the entire ring. The longer the period of the guard timer, the longer an Ethernet ring node is unaware of relevant new or existing requests transmitted from other Ethernet ring nodes, and therefore unable to react to them. A guard timer is used in every Ethernet ring node. Once a guard timer is started, it expires by itself. When the guard timer is not running, the R-APS request/state and status information is forwarded unchanged.

WTR Time

The Wait To Restore timing value to be used in revertive switching. You can set the WTR period to **1** minute or from **5-12** minutes in 1 minute steps. The default value is **5** minutes. In revertive mode, the wait to restore (WTR) timer is used to prevent frequent operation of the protection switching due to intermittent signal failure defects.

Hold Off Time

The timing value to be used to make persistent check on Signal Fail (SF) before switching. The Hold off timer valid range is 0 to 10 seconds in steps of 100 ms. The default is 0.

The holdoff timer is used to allow, for example, a server layer protection switch to have a chance to fix the problem before switching at a client layer, in order to coordinate timing of protection switches at multiple layers. When a new defect or more severe defect occurs (new SF), this event is not reported immediately to protection switching if the provisioned holdoff timer value is non-zero.

Instead, the holdoff timer is started. When the holdoff timer expires, the trail that started the timer is checked as to whether a defect still exists. If one does exist, that defect is reported to protection switching. The reported defect need not be the same one that started the timer.

Version

Select v1 or v2 as the ERPS version to be used. For fields such as Version, OpCode, Flags, and End TLV, the values used are as defined in ITU-T Y.1731 (Version 0x01 is transmitted per the current version of this Recommendation at the time of this publication.) G.8032v1 supported a single ring topology and G.8032v2 supports multiple rings/ladder topology.

v1: G.8032 v1 supported a single ring topology. The v1 protocol is robust enough to work for unidirectional failure and multiple link failure scenarios in a ring topology. It allows mechanism to force switch (FS) or manual switch (MS) to take care of field maintenance scenario.

v2: G.8032 v2 supports multiple rings/ladder topology. The v2 protocol also introduced other features such as Revertive/ Non-revertive mode after condition, that is causing the switch, is cleared, Administrative commands - Forced Switch (FS), Manual Switch (MS) for blocking a particular ring port, Flush FDB (Filtering database), and support of multiple ERP instances on a single ring.

Revertive

Check the checkbox for Revertive mode operation. Uncheck the checkbox for NonRevertive mode operation. An Ethernet ring node that has one or more ring ports in an SF condition, upon detection of clearance of the SF condition, keeps at least one of these ring ports blocked for the traffic channel and for the R-APS channel, until the RPL is blocked as a result of Ethernet ring protection reversion, or until there is another higher priority request (e.g., an SF condition) in the Ethernet ring.

Revertive operation: When all ring links and Ethernet ring nodes have recovered and no external requests are active, reversion is the action to be taken.

Non-revertive operation: the Ethernet ring does not automatically revert when all ring links and Ethernet ring nodes have recovered and no external requests are active.

Both revertive and non-revertive handling are discussed in Rec. ITU-T G.8032/Y.1344 (03/2010). Protection switching on a manual switch request is completed when the specified actions are performed by each Ethernet ring node. At this point, the conditions are created to allow the traffic flows to be steered around the Ethernet ring.

VLAN config

You can click the [VLAN Config](#) hyperlink to display the ERPS VLAN Configuration for the port. See below for description.

RPL Configuration

The ring protection link is the ring link that under normal conditions (i.e., without any failure or request) is blocked (at one or both ends) for traffic channel, to prevent the formation of loops.

RPL Role

Select either `RPL_Owner` or `RPL_Neighbour`, where:

RPL Neighbour node, when configured, is an Ethernet ring node adjacent to the RPL that is responsible for blocking its end of the RPL under normal conditions (i.e., the ring is established and no requests are present in the ring) in addition to the block by the RPL owner node. However, the RPL Neighbor is not responsible for activating the reversion behavior.

RPL Owner node is an Ethernet ring node adjacent to the RPL that is responsible for blocking its end of the RPL under normal conditions (i.e., the ring is established and no requests are present in the ring).

It is also responsible for activating reversion behavior from protected or manual switch/forced switch (MS/FS) conditions.

RPL Port

This dropdown lets you select the east port or west port as the RPL block.

None: Nothing selected as the RPL block.

Port0: This selects the East port of the S4224 in the ring as the RPL block.

Port1: This selects the West port of the S4224 in the ring.

Clear

Clear: If the owner must be changed; check the Clear checkbox to clear the RPL owner for that ERPS ring.

Sub-Ring Configuration

Displays only for a “Sub” Ring type instance.

Ring Type

Displays “Sub” Ring or “Major” as the ring type for this instance.

Topology Change

Check this checkbox to cause topology changes in the sub-ring to be propagated to the Major ring. (This field only displays for a Ring Type of ‘Sub-Ring’. Topology change propagation, when enabled, sends a *Topology_Change* signal when a flush FDB action is triggered by the ERP Control Process of a Sub-Ring’s ERP Instance. The *Topology_Change* signal is disabled after a period of 10 ms.

ERPS Instance Command

Command

A port (e.g., Port0 or Port1) can be administratively configured to be in either **Manual** switch or **Forced** switch state or **None** (neither Forced or Manual) from the Command dropdown, or you can **Clear** the active local administrative selection.

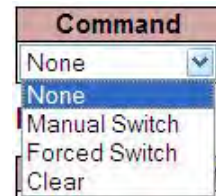
None (neither Forced or Manual) from the Command dropdown (the default).

Manual Switch: In the absence of a failure or FS, a Manual Switch selection forces a block on the ring port where the command is issued.

Forced switch: A Forced Switch (FS) selection forces a block on the ring port where the command is issued.

Clear: The Clear entry clears the active local administrative selection (e.g., Forced Switch or Manual Switch state). The Clear command is used for these operations:

- a) Clearing an active local administrative command (e.g., forced switch or manual switch),
- b) Triggering reversion before the WTR or WTB timer expires in case of revertive operation, and
- c) Triggering reversion in case of non-revertive operation.



Port

The port (**None**, **Port0** or **Port1**) to be administratively configured.

ERPS Instance State

Protection State

The current ERPS state according to State Transition Tables in G.8032.

Pending: The state is in the process of changing; you have selected a change but not yet 'Saved' the change.

Protected: ERPS protected mode is enabled for this instance.

None: No protected mode is enabled for this instance.

Idle: Protected mode is idle for this instance.

Forced Switch: this instance is in forced switch mode. A Forced Switch (FS) selection forces a block on the ring port where the command is issued.

Manual Switch: this instance is in manual switch mode. In the absence of a failure or FS, a Manual Switch selection forces a block on the ring port where the command is issued.

See "Ethernet linear protection switching - Recommendation ITU-T G.8031/Y.1342, Annex A" – State transition tables of protection switching Tables A.1 - A.6. These tables provide protection switching state transition information for various protection switching configurations (although Annex A does not form an integral part of the Recommendation). The states include, but are not necessarily limited to No request (NR), Lockout (LO), Forced switch (FS), Signal fail (W) SF, Signal fail (P) SF-P, Manual switch MS, Wait to restore WTR, Exercise EXER, Reverse request RR). Annex A notes that any other global or local request which is not described in the state transition tables does not trigger any state transition.

Port 0

OK: State of East port is ok.

SF: State of East port is Signal Fail.

Port 1

OK: State of West port is ok.

SF: State of West port is Signal Fail.

Transmit APS

The transmitted APS according to the State Transition Tables in G.8032. Signal Fail (SF) is declared when ETH trail signal fail condition is detected. No Request (NR) is declared when there are no outstanding conditions (e.g., SF, SF DNF BPR1, NR BPR0, etc.) on the node. See Rec. ITU-T G.8031/Y.1342 for details.

Port 0 Receive APS

The received APS for Port 0 according to State Transition Tables in G.8032.

Port 1 Receive APS

The received APS for Port 1 according to State Transition Tables in G.8032.

WTR Remaining

The remaining WTR (Wait to Restore) timeout in milliseconds.

RPL Un-blocked

APS is received on the working flow. Displays a green LED (●) for Up or a red LED (●) for Down.

No APS Received

RAPS PDU is not received from the other end. Displays a green LED (●) for Up or a red LED (●) for Down.

Port 0 Block Status

Block status for Port 0 (Both traffic and R-APS block status). The R-APS channel is never blocked on sub-rings without virtual channel enabled.

Blocked: the status for Port 0 (both traffic and R-APS block status) is 'blocked'.

Unblocked: the status for Port 0 (both traffic and R-APS block status) is 'unblocked'.

Port 1 Block Status

Block status for Port 1 (Both traffic and R-APS block status). The R-APS channel is never blocked on sub-rings without virtual channel enabled.

Blocked: the status for Port 1 (both traffic and R-APS block status) is 'blocked'.

Unblocked: the status for Port 1 (both traffic and R-APS block status) is 'unblocked'.

FOP Alarm

Displays the Failure of Protocol Defect (FOP) status. If FOP is detected, the red LED (●) displays in the table; the green LED (●) displays if FOP is not detected.

Due to errors in provisioning, the ERP Control Process may detect a combination of conditions which should not occur during "normal" conditions. To warn of such an event, a Failure of Protocol – Provisioning Mismatch (FOP-PM) is defined. The FOP-PM defect, detected if the RPL Owner Node receives one or more No Request R-APS messages with the RPL Blocked status flag set (NR, RB), and a Node ID that differs from its own. The ERP Control Process must notify the equipment fault management process when it detects such a defect condition, and will continue its operation as well as possible. This is only an overview of the defect condition. The associated defect and its details are defined in ITU-T G.8021 as amended by ITU-T G.8021 Amd.1 and Amd.2. Other than alarm noting the defect condition, the ERP state machine continues operation as well as possible.

Buttons

Save: Click to save changes.

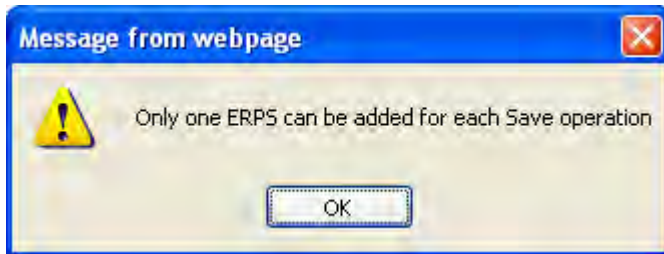
Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page immediately.

Auto-refresh: Click to automatically refresh the page every three seconds.

Messages

Message: Only one ERPS can be added for each Save operation



Meaning: An ERPS parameter was mis-configured.

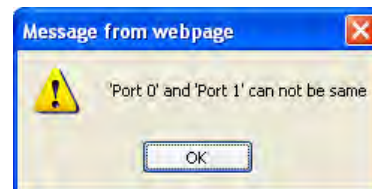
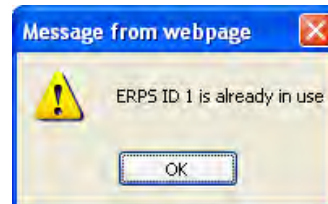
Recovery: 1. Click the OK button to clear the webpage message. 2. Configure an ERPS instance and then Save before adding another ERPS instance.

Message: ERPS ID x is already in use.

'Port x APS MEP' must be zero

'Port x SF MEP' must be zero

'Port 0' and 'Port 1' can not be the same



Meaning: An ERPS parameter was mis-configured when adding an ERPS instance.

Recovery: 1. Click the **OK** button to clear the webpage message. 2. Re-enter the invalid ERPS parameter. See the preceding section.

Ring Protection and MEP Configuration

The S4224 lets you configure the RPL port so it can act in the role of Owner or Neighbor on that ring instance. The WTR time and Hold off timer serve the same purpose as EPS. The Guard timer on the EPRS instance is configurable and helps in ignoring aged R-APS messages that circulate around the ring. The Ring ports have the Y.1731 MEPs which exchange CCMs to monitor the health of the link and also trigger signal failures that can cause the link failure and protection to activate.

MEP Configuration Refresh

Instance Data

| Instance | Domain | Mode | Direction | Residence Port | Flow Instance | Tagged VID | EPS Instance | This MAC |
|----------|--------|------|-----------|----------------|---------------|------------|--------------|-------------------|
| 1 | Port | Mep | Down | 1 | 1 | 0 | 1-2-4 | 00-C0-F2-56-19-09 |

Instance Configuration

| Level | Format | Domain Name | MEG id | MEP id | Tagged VID | VOE | cLevel | cMEG | cMEP | cAIS | cLCK | cSSF | aBLK | aTSF |
|-------|---------|-------------|---------------|--------|------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 0 | ITU ICC | | ICC000MEG0000 | 1 | 0 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Peer MEP Configuration

| Delete | Peer MEP ID | Unicast Peer MAC | cLOC | cRDI | cPeriod | cPriority |
|--------------------------|-------------|-------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> | 1 | 00-00-00-00-00-00 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Add New Peer MEP

Functional Configuration

| Continuity Check | | | APS Protocol | | | | |
|--------------------------|----------|------------|--------------------------|----------|-------|-------|------------|
| Enable | Priority | Frame rate | Enable | Priority | Cast | Type | Last Octet |
| <input type="checkbox"/> | 7 | 1f/sec | <input type="checkbox"/> | 7 | Multi | L-APS | 1 |

Fault Management Performance Monitoring

Save Reset

The screen above shows a MEP configured with R-APS as the APS Protocol Type. See the “[MEP Configuration](#)” section on page 213 for more information.

Ring Protection Conditions and Commands

The S4224 supports the Ethernet ring **SF** and **NR** conditions per Rec. ITU-T G.8032/Y.1344 (03/2010).

Signal fail (SF) - When an SF condition is detected on a ring link, and it is determined to be a "stable" failure, Ethernet ring nodes adjacent to the failed ring link initiate the protection switching mechanism described in the ITU Recommendation.

No request (NR) - The condition when no local protection switching requests are active.

The **FS**, **MS**, and **Clear** administrative commands are supported:

Forced switch (FS) - This command forces a block on the ring port where the command is issued.

Manual switch (MS) - In the absence of a failure or FS, this command forces a block on the ring port where the command is issued.

Clear - The Clear command is used for these operations:

- Clearing an active local administrative command (e.g., Forced switch or Manual switch).
- Triggering reversion before the WTR or WTB timer expires in case of revertive operation.
- Triggering reversion in case of non-revertive operation.

Note that at the time of this publication, other commands (Lockout of protection, Replace the RPL, Exercise signal) are undergoing further ITU-T study.

ERPS VLAN Configuration

VLAN config: click the [VLAN Config](#) link in the ERPS Instance Configuration table to display the related ERPS VLAN Configuration page.

ERPS VLANs are used because Ethernet ring protection configured as a single instance only works at the physical level (adjacent nodes must be directly connected). The ring protection operates at the interface (port) level and not at the VLAN level.

The VLANs created here are tied to Ring instances that are like traffic channels that contain different sets of VLANs. A ring instance is responsible for the protection of a subset of VLANs that transport traffic over the physical ring.

When ring instances are configured for the ring, each ring instance should have its own RPL owner, an east and a west interface, and a ring protection link end.

Click the **Add New Entry** button to display the ERPS VLAN Configuration page.

| Delete | VLAN ID |
|--------|---------|
| Delete | 0 |

Buttons: Add New Entry, Back, Save, Reset, Refresh

Enter a new ERPS VLAN ID. The default is 0. The valid range is 1-4094. Click the **Save** button when done.

Add one or more new VLAN IDs as required.

| Delete | VLAN ID |
|--------------------------|---------|
| <input type="checkbox"/> | 100 |
| <input type="checkbox"/> | 200 |
| <input type="checkbox"/> | 300 |

Buttons: Add New Entry, Back, Save, Reset, Refresh

The example above shows ERPS VLAN Configuration 3 with VLAN IDs 100, 200 and 300 configured.

Add a New ERPS Protection Group Procedure

1. Navigate to the **Configuration > ERPS** menu path. The ERPS table displays.
2. Click the **Add New Protection Group** button. Entry fields display for the new Protection Group.
3. Enter unique parameters for ERPS ID, Port 0, Port 1, Port 0 APS MEP, Port 1 APS MEP, Port 0 SF MEP, and Port 1 SF MEP.
4. At the **Ring Type** dropdown, select **Major** or **Sub**.
5. Check or uncheck the **Interconnected Node** and **Virtual Channel** checkboxes.
6. Enter a **Major Ring ID** (only applies if **Ring Type = Sub** was selected in step 4 and **Interconnected Node** was checked in step 5).
7. When done click the **Save** button.
8. Repeat steps 2-7 for each new Protection Group to be added.
9. Verify your ERPS configuration (e.g., ERPS IDs 1, 2, 3, and 4 shown below).

Delete an Existing ERPS Protection Group Procedure

1. To delete an existing ERPS, check its checkbox in the **Delete** column.
2. Click the **Save** button.
3. Verify that the selected ERPS instance(s) are deleted from the table. Click the **Refresh** button if necessary.

The ERP instance is an entity that is responsible for the protection of a subset of the VLANs that transport traffic over the physical Ethernet ring. Each ERP instance is independent of other ERP instances that may be configured on the physical Ethernet ring. The S4224 implements the ITU G.8032 standard for ERPS, which uses the APS automatic protection protocol for protection in ring and interconnected ring topology. The S4224 supports G.8032v1 in a single ring topology and G.8032v2 in multiple rings/ladder topologies.

ERPS specifies protection switching mechanisms and a protocol for Ethernet layer network (ETH) rings. Ethernet Rings can provide wide-area multipoint connectivity more economically due to their reduced number of links. The mechanisms and protocol defined in this Recommendation achieve highly reliable and stable protection; and never form loops, which would fatally affect network operation and service availability.

Each Ethernet Ring Node is connected to adjacent Ethernet Ring Nodes participating in the same Ethernet Ring, using two independent links. A ring link is bounded by two adjacent Ethernet Ring Nodes, and a port for a ring link is called a ring port. The minimum number of Ethernet Ring Nodes in an Ethernet Ring is two.

The ring protection switching architecture fundamentals are a) the principle of loop avoidance, and b) the use of learning, forwarding, and Filtering Database (FDB) mechanisms defined in the ETH_FF (Ethernet Flow Forwarding function).

Loop avoidance in an Ethernet Ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the Ring Protection Link (RPL), and under normal conditions this ring link is blocked (i.e., not used for service traffic). One designated Ethernet Ring Node, the 'RPL Owner Node', is responsible for blocking traffic at one end of the RPL. Under an Ethernet ring failure condition, the RPL Owner Node is responsible for unblocking its end of the RPL (unless the RPL has failed) allowing the RPL to be used for traffic. The other Ethernet Ring Node adjacent to the RPL, the 'RPL Neighbour Node', may also participate in blocking or unblocking its end of the RPL. The event of an Ethernet Ring failure results in protection switching of the traffic. This is achieved under the control of the

ETH_FF functions on all Ethernet Ring Nodes. An APS protocol is used to coordinate the protection actions over the ring.

Note: The SOAM MEP configuration must be successfully completed before configuring Ethernet Ring Protection Switching (ERPS) using the functions in this section. See “[MEP Configuration](#)” on page 315.

ERPS Parameters Summary

ERPS instances can be created using the basic parameters below:

| Configurable Parameter | Valid Range | Default |
|--|---------------------|---------|
| ERPS Id | 1-64 | 1 |
| Port 0 (East port) | Valid port range | 1 |
| Port 1 (West Port) | Valid port range | 1 |
| | Port 0 SF MEP 1-32 | 1 |
| | Port 1 SF MEP 1-32 | 1 |
| | Port 0 APS MEP 1-32 | 1 |
| | Port 1 APS MEP 1-32 | 1 |
| | Ring type Major/Sub | Major |
| Interconnected Node | Yes/No | No |
| Virtual Channel | Yes/No | No |
| Major Ring Id (Interconnected Sub ring) | 0-99 | 0 |

Individual instances have following configurable parameters:

| Configurable Parameter | Valid Range | Default |
|-------------------------------|------------------------------------|---------|
| Instance Configuration | | |
| Guard Time | 10ms-2000ms, in steps of 10 ms | 500 ms |
| WTR Time | 1min, 5min - 12min | 1 min |
| Hold Off Time | 0ms - 10000ms, in steps of 100ms | 0 ms |
| Version | v1/v2 | v2 |
| Revertive | Enable/Disable | Enable |
| VLAN Config | | |
| VLAN ID | 1-4094 | N/A |
| RPL Configuration | | |
| Role | None / RPL_Owner / RPL_Neighbour | None |
| Port | Port0 / Port1 | None |
| Instance Command | | |
| Command | None, Manual Switch, Forced Switch | None |
| Port | Port0 / Port1 | None |

MAC Address Table Configuration

The S4224 **Configuration > MAC Table** menu path supports MAC Address table configuration in terms of Aging Configuration, MAC Table Learning, and Static MAC table Configuration.

Switching of frames is based on the DMAC address contained in the frame. The S4224 builds up a table that maps MAC addresses to S4224 ports for knowing to which ports the frames should go, based on the DMAC (Destination MAC) address in the frame. This table contains both static and dynamic entries.

The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and S4224 ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC (Source MAC) address is used by the S4224 to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address, have been seen after the configured Aging Time.

Enabling known MAC address traffic involves port security. Port security can be either 'static' or 'dynamic'.

Static port security lets you specify which devices are allowed access through a given port. This is done manually by entering the "allowed" device MAC addresses in the MAC address table. Static port security is also known as "MAC address filtering".

Dynamic port security is similar, but instead of specifying the MAC address of the devices, you specify the maximum number of devices to be allowed on the port. If the maximum number that you specify is more than the number of MAC addresses specified manually, the switch learns the MAC address automatically, up to the maximum specified. If the maximum number specified is less than the number of MAC addresses already specified statically, an error message displays.

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging

Aging Time seconds

MAC Table Learning

| | Port Members | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| Auto | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> |
| Disable | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Secure | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Static MAC Table Configuration

| | Port Members | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------------------|--------------|-------------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| Delete | VLAN ID | MAC Address | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| Add New Static Entry | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Save Reset | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

Aging Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds (5 minutes). This removal is called 'aging'.

Disable Automatic Aging

Check the checkbox to disable aging.

Aging Time

The FDB is configured with aging time for dynamic learned entries in 1 second increments with the lowest being 10 seconds to a maximum of 1000000 seconds (11.57 days). The default value is 5 minutes (300 seconds). Aging can be disabled by setting the aging time to 0. Note that when aging is disabled, the FDB size can grow to a maximum of 8000 entries. After the maximum limit of the MAC limit is reached, the new MAC entries are added and the older dynamic MAC entries are purged from the database.

Configure aging time by entering a value here in seconds; for example, **Aging Time 300 seconds** in the screen sample above. The valid values are 0 and 10 - 1000000 seconds (11.57 days).

Disable the automatic aging of dynamic entries by checking the **Disable Automatic Aging** checkbox.

MAC Table Learning

All S4224 learning and switching is based on the MAC forwarding and filtering database (FDB). The S4224 web interface provides a way to purge all dynamic-only or static and dynamic entries out of the FDB. The S4224 FDB can be configured with static MAC entries for filtering or forwarding. The static entries are not aged out and remain in the device even after a power cycle. The Management interface provides options to add, edit, and delete static entries. Up to 1000 static entries can be stored. Each static entry also has an associated priority which will be used for QoS. See the ['QoS Configuration'](#) section on page 312 for details on user priority setting.

Bridge ports can be configured to be enabled or disabled for MAC forwarding. When the port is in disabled state, no learning/forwarding takes place. MAC Table Learning can be set to Auto, Disable, or Secure. This information is only available on this page. The MAC Table Learning setting is stored and will be restored after a power cycle.

Per IETF RFC 2233 section 3.1.13, if a port is administratively down, the operational state of the port is also brought down and is not a fault condition. If the administrative state is up but the operational state is down, it implies a fault, and a notification must be sent.

If the learning mode for a given port is grayed out, another module has control of the mode, so that it cannot be changed by a user. An example of such a module is the MAC-based Authentication under 802.1X.

Ports can do learning based on these settings:

Auto

If selected, learning is done automatically as soon as a frame with an unknown SMAC (Source MAC address) is received.

Disable

No learning is done if selected.

Secure

If selected, only static MAC entries are learned, all other frames are dropped.

Note: Make sure that the link used for managing the S4224 is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the S4224 via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown here. The static MAC table can contain up to 64 entries.

The MAC table is sorted first by VLAN ID and then by MAC address.

Delete

Check to delete the entry. It will be deleted during the next Save.

VLAN ID

The VLAN ID of the entry. Each new line (VLAN entry) must have a unique VLAN ID.

MAC Address

Displays the assigned MAC address of the entry.

Port Members

Check one or more checkboxes to indicate which port(s) are members of the entry. Check or uncheck as needed to modify the entry. **Note:** If none are checked, the MAC addresses for all ports will be blocked.

Add New Static Entry

Click the **Add New Static Entry** button to add a new entry to the static MAC table.

Configuration

- System
- Ports
- DHCP
- Security
- Aggregation
- Link OAM
 - Loop Protection
- Spanning Tree
- IPMC Profile
 - MVR
 - IPMC
 - LLDP
 - EPS
 - MEP
 - ERPS
 - MAC Table**
 - VLAN Translation
 - VLANs
 - Private VLANs
 - VCL
 - Ethernet Services
 - Performance Monitor
 - QoS
 - Mirroring
 - PTP
 - GVRP

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging

Aging Time seconds

MAC Table Learning

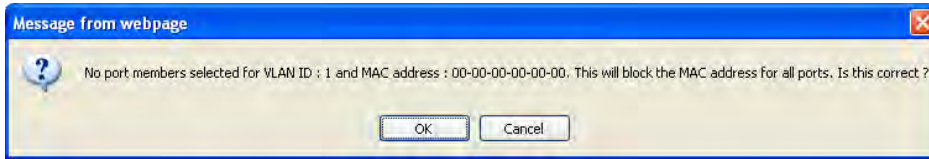
| | Port Members | | | | | |
|---------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| Auto | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Disable | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Secure | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Static MAC Table Configuration

| Delete | VLAN ID | MAC Address | Port Members | | | | | |
|--------|--------------------------------|--|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| | | | 1 | 2 | 3 | 4 | 5 | 6 |
| Delete | <input type="text" value="1"/> | <input type="text" value="00-00-00-00-00-00"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Specify the VLAN ID (1-4094), MAC address, and Port Members included for the new MAC entry.

Note: If you do not select any Port Members and then click the **"Save"** button, a message displays warning you that this will block the MAC address for all ports.



If this is the configuration you want, click the **OK** button. Otherwise click the **Cancel** button and select one or more Port Members.

Click the "Save" button when done.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

VLAN Translation Configuration

The S4224 lets you configure VLAN translation (mapping) from the **Configuration > VLAN Translation Configuration** menu path. Here you can configure the **Port to Group Mapping** and the **VID Translation Mapping** functions.

Port to Group Mapping

Click the “**Add New Entry**” button to display the entry line of the Port to Group mapping Table. This page lets you configure switch Ports to use a given VLAN Translation Mapping Group. This will enable all VLAN Translation mappings of that group (if any) on the selected switch port.

| Port | Group Configuration | |
|------|--------------------------|----------|
| | Default | Group ID |
| * | <input type="checkbox"/> | <> |
| 1 | <input type="checkbox"/> | 1 |
| 2 | <input type="checkbox"/> | 2 |
| 3 | <input type="checkbox"/> | 3 |
| 4 | <input type="checkbox"/> | 4 |
| 5 | <input type="checkbox"/> | 5 |
| 6 | <input type="checkbox"/> | 6 |
| 7 | <input type="checkbox"/> | 7 |
| 8 | <input type="checkbox"/> | 8 |
| 9 | <input type="checkbox"/> | 9 |
| 10 | <input type="checkbox"/> | 10 |
| 11 | <input type="checkbox"/> | 11 |

The displayed settings are explained below.

Port

The Port column shows the list of ports for which you can configure the VLAN Translation Mapping Group.

Default

To set the switch port to use the default VLAN Translation Group click the checkbox and press Save.

Group ID

The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch.

A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from 1 to 6.

Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page immediately.

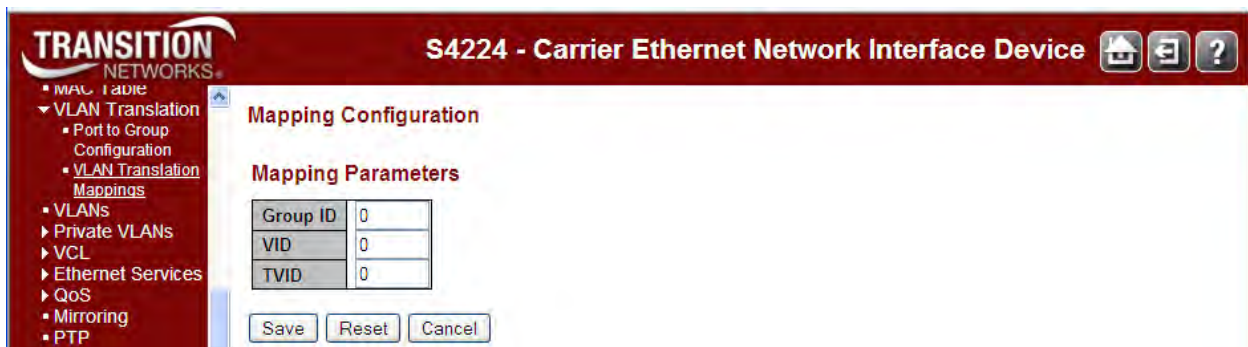
Auto-refresh: Click to automatically refresh the page every three seconds.

VLAN Translation Mapping

S4224 VID Translation Mapping is done from the **Configuration > VLAN Translation > VID Translation Mapping** menu path. This page lets you create mappings of VLANs to Translated VLANs and organize these mappings into global Groups.



The VLAN Translation Table initially displays an empty table. Click the “+” icon to display the VLAN Translation Mapping Table entry fields.



The displayed VLAN Translation Mapping Table settings are explained below.

Group ID

The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch.

A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group. A valid Group ID is an integer value from **1** to **28**.

Note: By default, each port is set to use the group with Group ID (GID) equal to the port number. For example, S4224 Port 1 is by default set to use the group with GID = 1.

VID




Indicates the VLAN of the mapping (i.e. 'source' VLAN). A valid VLAN ID ranges from 1 to 4095.

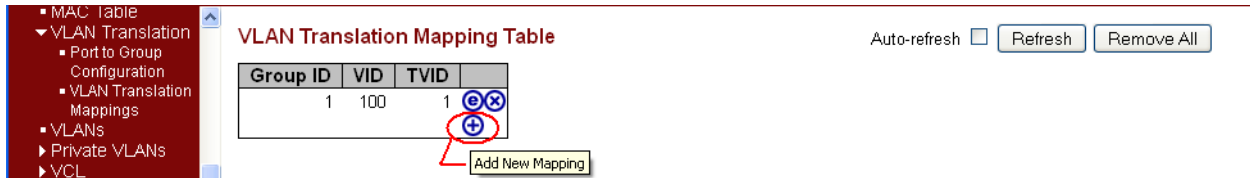
TVID

Indicates the VLAN ID to which VLAN ID of an ingress frame will be translated to (granted that the mapping is enabled on the ingress port that the frame arrived at). A valid VLAN ID ranges from 1 to 4095.



Modification Buttons

You can modify each VLAN Translation mapping in the table using the following buttons:

- : Edits the mapping row.
- : Deletes the mapping.
- : Adds a new mapping.



The screenshot shows the 'VLAN Translation Mapping Table' interface. On the left is a navigation menu with options like 'MAC Table', 'VLAN Translation', 'Port to Group Configuration', 'VLAN Translation Mappings', 'VLANs', 'Private VLANs', and 'VCL'. The main area contains a table with the following data:

| Group ID | VID | TVID | |
|----------|-----|------|---|
| 1 | 100 | 1 |   |

Below the table is a red-bordered button labeled 'Add New Mapping'. Above the table are three buttons: 'Auto-refresh' (with a checkbox), 'Refresh', and 'Remove All'.

Buttons

Auto-refresh: Click to automatically refresh the page every three seconds.

Refresh: Click to refresh this page immediately.

Remove All: Click to remove all VLAN Translation mappings. At the confirm prompt, click **OK** to proceed.

VLANs Configuration

The S4224 lets you configure VLANs from the **Configuration > VLANs** menu path. Here you can configure the 'VLAN Membership' and the 'Ports' sub-menu functions.

IEEE 802.1Q standard VLANs are supported and the default configuration is as follows:

- All ports are VLAN aware.
- All ports are members of VLAN 1.
- The switch management interface is on VLAN 1.
- All ports have a Port VLAN ID (PVID) of 1.
- All ports can send and receive both VLAN-tagged and untagged packets. In the default configuration, any port is able to send traffic to any other port, and a PC connected to any port will be able to reach the management interface.

Broadcast traffic, for example, will be flooded to all ports on the switch.

Note: VLAN ID 1 is always reserved for the default VLAN. The range of the VLAN ID is (2 to 4095).

| Port | Mode | Port VLAN | Port Type | Ingress Filtering | Ingress Acceptance | Egress Tagging | Allowed VLANs | Forbidden VLANs |
|------|--------|-----------|-----------|-------------------------------------|---------------------|----------------|---------------|-----------------|
| * | <> | 1 | <> | <input checked="" type="checkbox"/> | <> | <> | 1 | |
| 1 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 2 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 3 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 4 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 5 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 6 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 7 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 8 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 9 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 10 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |
| 11 | Access | 1 | C-Port | <input checked="" type="checkbox"/> | Tagged and Untagged | Untag All | 1 | |

This page allows for controlling VLAN configuration on the switch. The page is divided into a global section and a per-port configuration section.

Global VLAN Configuration

Allowed Access VLANs

This field shows the allowed Access VLANs (i.e., it only affects ports configured as Access ports). Ports in other modes are members of all VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.

The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: `1,10-13,200,300`. Spaces are allowed in between the delimiters.

Ethertype for Custom S-ports

This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports.

The setting is in force for all ports whose **Port Type** is set to S-Custom-Port. It takes effect on the egress side. The format of 'Ether Type' is restricted to 0x600 - FFFF.

Port VLAN Configuration

Port

This is the logical port number of this row.

Mode

The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below. Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port will get when the mode is applied.

Access: Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:

- Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1.
- Accepts untagged and C-tagged frames.
- Discards all frames that are not classified to the Access VLAN.
- On egress all frames classified to the Access VLAN are transmitted untagged. Other (dynamically added VLANs) are transmitted tagged.

Trunk: Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:

- By default, a trunk port is member of all VLANs (1-4094).
- The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs
- Frames classified to a VLAN that the port is not a member of are discarded.
- By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress.
- Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress.

Hybrid: Hybrid ports resemble trunk ports in many ways, but have additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:

- Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware.
- Ingress filtering can be controlled.
- Ingress acceptance of frames and configuration of egress tagging can be configured independently.

Port VLAN

Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 - 4094, default being 1.

On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).

On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.

The Port VLAN is called an "Access VLAN" for ports in Access mode and "Native VLAN" for ports in Trunk or Hybrid mode.

Port Type

Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.

Unaware: On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.

C-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.

S-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag.

S-Custom-Port: On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.

Ingress Filtering

Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.

If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.

If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

Ingress Acceptance

Hybrid ports allow for changing the type of frames that are accepted on ingress.

Tagged and Untagged: Both tagged and untagged frames are accepted.

Tagged Only: Only tagged frames are accepted on ingress. Untagged frames are discarded.

Untagged Only: Only untagged frames are accepted on ingress. Tagged frames are discarded.

Egress Tagging

Ports in Trunk and Hybrid mode may control the tagging of frames on egress.

Untag Port VLAN: Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.

Tag All: All frames, whether classified to the Port VLAN or not, are transmitted with a tag.

Untag All: All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.

Allowed VLANs

Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be members of one VLAN, the Access VLAN.

The field's syntax is identical to the syntax used in the [Forbidden VLANs](#) field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to **1-4094**.

The field may be left empty, which means that the port will not become member of any VLANs.

Forbidden VLANs

A port may be configured to never be a member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.

The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the [Allowed VLANs](#) field.

By default, the field is left blank, which means that the port may become a member of all possible VLANs.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Provider Bridging (IEEE 802.1ad 2005)

The S4224 is compliant with IEEE802.1ad 2005 standard in recognizing S-Tags and C-Tags. The S4224 can recognize S-Tag or C-Tag based on Ethertype. The default value is 0x88a8 for S-Tag and 0x8100 for C-Tag as per the standard. You can configure the Ethertype of S-Tag via the web interface. A default list of 0x88a8, 0x8100 and 0x9100 is provided on the web interface.

| Tag Type | Name | Value |
|-------------------|--|-------|
| Customer VLAN tag | IEEE 802.1Q Tag Protocol Type (802.1Q Tag Type) | 8100 |
| Service VLAN tag | IEEE 802.1Q Service Tag Type (802.1Q S-Tag Type) | 88A8 |
| Q-in-Q | VLAN Tag Protocol Identifier | 9100 |

Figure 4. 802.1Q EtherTypes (excerpt from IEEE 802.1ad 2005)

The S4224 can be an SVLAN bridge, C-bridge, or both bridge types, and the hardware can support inspection of both the tags. The S4224 can push and pop one or both tag types.

Provider Tagging Use cases

1. **All to one bundling services:** In this scenario the device caters to multi-tenant services. This service is the Ethernet private line as stated by the MEF 30 standard.

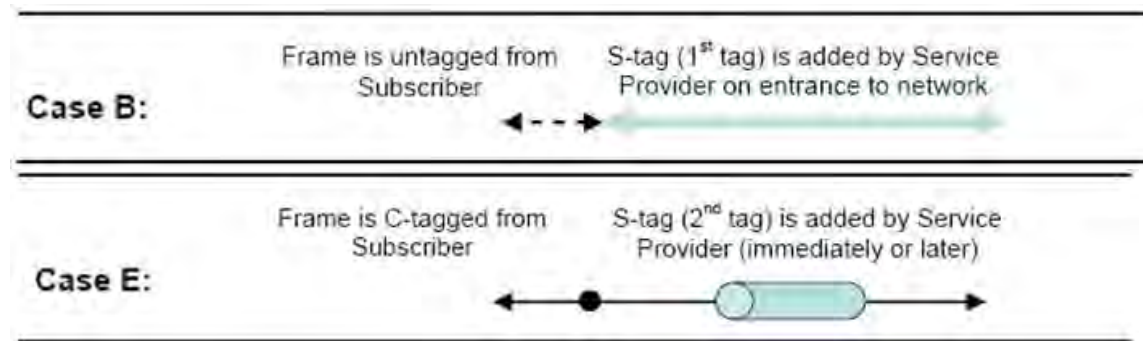


Figure 5. All to one bundling VLAN Cases

All traffic from customer facing ports is bundled using an S-VLAN tag. The SVID will identify the customer traffic within the provider network; at the hand-off on the other side of the network, the S-tag is stripped. The customer traffic can be Untagged, Priority tagged or C-VLAN tagged; in some cases it can be all. The provider S-tag bundles all transparently based on the ingress port and transported through the provider network, hence the name 'all to one bundling'.

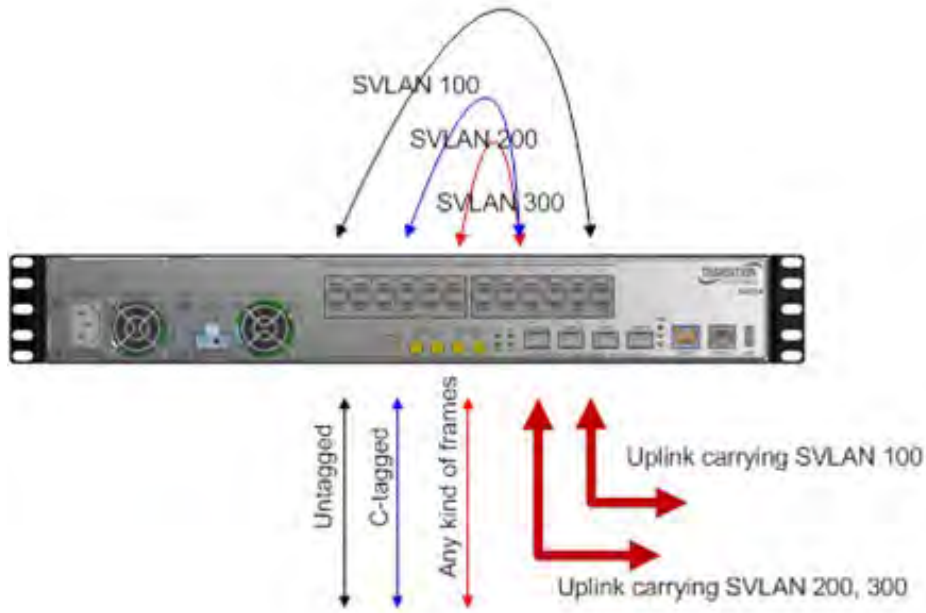


Figure 6. S-VLAN with multiple trunks (EPL service at 3 different UNIs)

2. Another case is shown below, with one S-Tag uplink or S-Tag trunk.

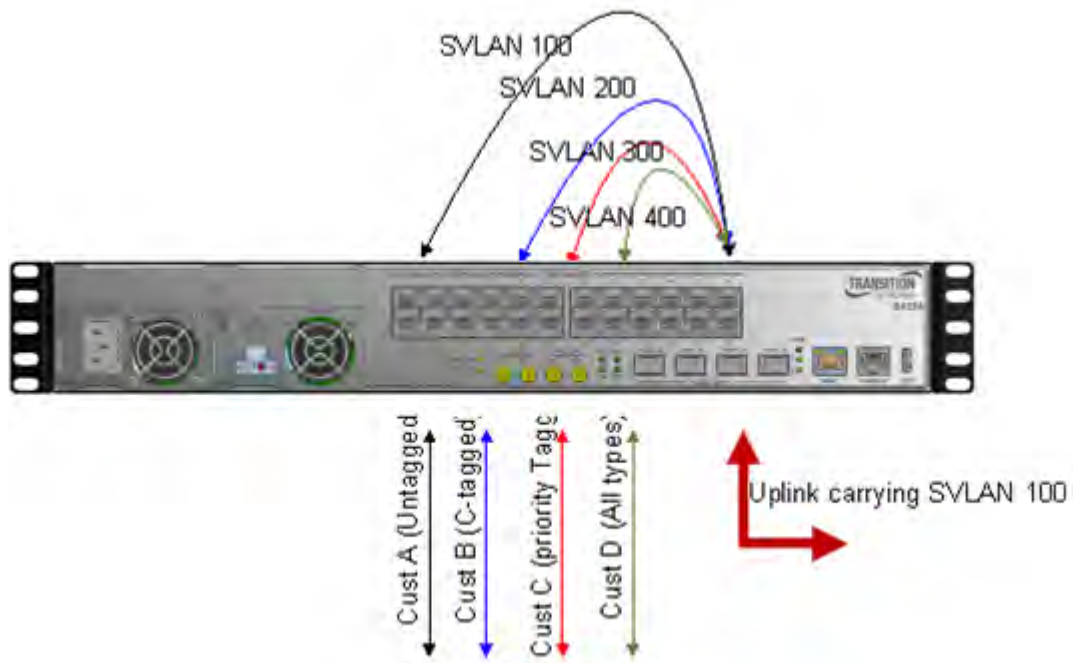


Figure 7. S-VLAN with one trunk (Multiple UNI bundled at the Operator domain)

Private VLANs Configuration

The S4224 lets you configure Private VLANs from the **Configuration > Private VLANs** menu path. Here you can configure the 'PVLAN Membership' and the 'Port Isolation' sub-menu functions. In a private VLAN, PVLANS provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN can not communicate with each other. Member ports of a PVLAN can communicate with each other.

PVLAN Membership

S4224 Private VLAN membership configuration can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

From the default page, click the “**Add New Private VLAN**” button to display the entry table.

| Delete | PVLAN ID | Port Members | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------------|----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| <input type="checkbox"/> | 1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> | 0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

This page lets you:

- Monitor and modify S4224 Private VLAN membership configurations,
- Add or delete Private VLANs, and
- Add or delete Private VLAN Port Members.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

The VLAN Port configuration table parameters are explained below.

Delete

To delete a private VLAN entry, check this checkbox. The entry will be deleted during the next Save.

PVLAN ID

Indicates the ID of this particular private VLAN. Enter a number from 2-28. The default, PVLAN ID 1, has all of the Port Members checked. When you add PVLAN IDs 2-6, the Port Member checkboxes are all unchecked by default.

Port Members

Displays a row of checkboxes for each port for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked.

By default, no PVLAN ID ports are members, and all checkboxes are unchecked when adding a new PVLAN. At least one port must be selected (checked) to add an entry.

Member ports of a PVLAN can communicate with each other. Isolated ports configured as part of a PVLAN cannot communicate with each other.

Add New Private VLAN

Click the **Add New Private VLAN** button to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the S4224 port number range. Any values outside this range are not accepted, and a warning message appears. Click **"OK"** to discard the incorrect entry, or click **"Cancel"** to return to the editing and make a correction.

The Private VLAN is enabled when you click the **"Save"** button.

You can use the **Delete** button to undo the addition of new Private VLANs.

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Example

When done, verify your **Configuration > Private VLANs > PVLAN Membership** config. For example, the screen below shows a PVLAN Membership configured with four PVLAN IDs (1, 10, 26, and 28).

The screenshot shows the 'Private VLAN Membership Configuration' interface. At the top right, there is an 'Auto-refresh' checkbox (unchecked) and a 'Refresh' button. Below this is a table with columns for 'Delete', 'PVLAN ID', and 'Port Members' (ports 1-28). The table contains four rows for PVLAN IDs 1, 10, 26, and 28. Row 1 has all port checkboxes checked. Row 10 has ports 2, 3, 4, and 5 checked. Row 26 has ports 2, 3, 6, and 7 checked. Row 28 has ports 2, 3, and 4 checked. Below the table are buttons for 'Add New Private VLAN', 'Save', and 'Reset'.

| Delete | PVLAN ID | Port Members | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------------|----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| <input type="checkbox"/> | 1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> | 10 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | 26 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | 28 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Port Isolation

You can configure port isolation from the **Configuration > Private VLANs > Port Isolation** menu path.

This page is used for enabling or disabling port isolation on ports in a Private VLAN. Port isolation offers isolation of that Port from the VLAN forwarding on the VLAN that it is a member of.

| Port Isolation Configuration | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Port Number | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Auto-refresh Refresh

Save Reset

A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Port Members

A checkbox is provided for each port of a private VLAN.

- When checked, port isolation is enabled on that port, and that port is considered “isolated”. Isolated ports configured as part of a PVLAN cannot communicate with each other.
- When unchecked, port isolation is disabled on that port, and that port is considered a “member port”. Member ports of a PVLAN are not isolated and can communicate with each other.

By default, port isolation is disabled (unchecked) on all ports (i.e., all ports are “member ports” at default).

Note: At least one port entry must be selected in order to add a new entry.

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

VCL (VLAN Control List)

The **Configuration > VCL (VLAN Control List)** menu path lets you configure the S4224 for MAC-based VLAN mappings and Protocol-based VLAN mapping. A VCL is used for assigning a particular flow to a particular VLAN. VCLs can enforce VLAN security that is based on a variety of information.

The IND-328x VCL (VLAN Control List) commands let you configure the IND-328x for MAC-based VLAN, Protocol-based VLAN, and/or IP Subnet-based VLAN mappings.

MAC-based VLANs let you add and delete MAC-based VLAN entries and assign the entries to different ports. This page shows only static entries.

Protocol-based VLANs let you configure the S4224 for Protocol-to-Group and/or Group-to-VLAN settings.

IP Subnet-based VLANs let you define a VLAN membership by the subnet to which a device's IP address belongs. You can add, update, and delete IP subnet-based VLAN entries and assign the entries (membership) to different ports. VLANs are layer 2 constructs, compared with IP subnets which are layer 3 constructs. In an environment employing VLANs, a one-to-one relationship often exists between VLANs and IP subnets, but it is possible to have multiple subnets on one VLAN. VLANs and IP subnets provide independent Layer 2 and Layer 3 constructs that map to each other, and this correspondence helps in network design. Note that this involves only static entries.

Note: Protocol-based VLANs and IP Subnet-based VLANs work only on untagged and priority tagged frames, while MAC based VLANs work on all kinds of frames.

MAC-based VLAN

The MAC-based VLAN entries can be configured here. This page lets you add and delete MAC-based VLAN entries and assign the entries to different ports. This page shows only static entries.

Click the **Add New Entry** button to display the entry fields.

The screenshot shows the web interface for the S4224 - Carrier Ethernet Network Interface Device. The main content area is titled "MAC-based VLAN Membership Configuration". It features a table with the following structure:

| Delete | MAC Address | VLAN ID | Port Members | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------------|-------------------|---------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | |
| <input type="checkbox"/> | 00-00-00-00-00-00 | 1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Below the table, there is an "Add New Entry" button, and at the bottom, "Save" and "Reset" buttons.

The MAC-based VLAN entries are explained below.

Delete

To delete a MAC-based VLAN entry, check this box and click the 'Save' button. The selected entry will be deleted.

MAC Address

Enter the MAC address in the format `xx-xx-xx-xx-xx-xx`.

VLAN ID

Enter the VLAN ID (VID).

Port Members

A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box (✓). To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked (□). By default, no ports are members, and all boxes are unchecked. At least one port must be checked to add an entry before you click the 'Save' button.

Add New Entry (MAC-based VLAN Member)

Click the **Add New Entry** button to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4094.

The MAC-based VLAN entry is enabled when you click the "Save" button. A MAC-based VLAN without any port members will be deleted when you click the "Save" button.

The **Delete** button can be used to undo the addition of new MAC-based VLANs.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Refresh: Refreshes the displayed table.

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

|<<: Updates the table starting from the first entry in the MAC-based VLAN Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

Example

The example below shows two MAC-based VLAN Membership configurations.

| MAC-based VLAN Membership Configuration | | | Port Members | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|-------------------|---------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Delete | MAC Address | VLAN ID | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| <input type="checkbox"/> | 00-00-00-00-00-00 | 1 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | aa-88-09-0d-0f-ee | 2 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |

In this example:

VLAN ID 1 has MAC address 00-00-00-00-00-00 with ports 1 and 6 as Port Members.

VLAN ID 2 has MAC address aa-88-09-0d-0f-ee with ports 2 - 5 as Port Members.

None of the ports are "forbidden".

Protocol-based VLAN

The **Configuration > VCL > Protocol-based VLAN** menu path lets you configure the S4224 for Protocol to Group and/or Group to VLAN settings.

Protocol to Group

This page lets you add new protocols to Group Name (unique for each Group) mapping entries and lets you view and delete already mapped entries for the S4224. At default, the table displays “No Group entry found!”.

Click the **Add New Entry** button to display the entry fields.

The screenshot shows the web interface for the S4224 - Carrier Ethernet Network Interface Device. The left sidebar contains a navigation menu with options like VCL, MAC-based VLAN, Protocol-based VLAN, and Ethernet Services. The main content area is titled "Protocol to Group Mapping Table" and features a table with columns for Delete, Frame Type, Value, and Group Name. A single entry is shown with Frame Type set to "Ethernet" and Value set to "Etype: 0x0800". Below the table are buttons for "Add New Entry", "Save", and "Reset". There is also an "Auto-refresh" checkbox and a "Refresh" button.

The displayed settings are explained below.

Delete

To delete a Protocol to Group Name map entry, check this checkbox. The entry will be deleted on the S4224 at the next 'Save'.

Frame Type

The different frame types have different formats and MTU values, but can coexist on the same physical medium. Select a 'Frame Type' of one of the following values from the dropdown:

Ethernet : the frame type is Ethernet. An Etype value and a Group Name entry are required. The Ethernet frame (the most common type, used directly by the IP).

SNAP : Subnetwork Access Protocol (SNAP) frame. Ethernet SNAP is similar to 802.2 with LLC parameters, but with expanded LLC capabilities. Ethernet SNAP can support IPX/SPX, TCP/IP, and AppleTalk Phase 2 protocols.

LLC : IEEE 802.2 Logical Link Control (LLC) frame. LLC addressing involves LLC protocol data units (PDUs) which contain addressing information, consisting of two fields; the Destination Service Access Point (DSAP) address field, and the Source Service Access Point (SSAP) address field. Each of these is an 8-bit field made up of two components.

Note: On changing the Frame type field, the valid values of the following text field will vary depending on the new frame type you select here.

Value

The valid value that you can enter in this text field depends on the option selected from the preceding 'Frame Type' selection menu. The criteria for the three Frame Types are explained below.

1. **Ethernet**: Values in the text field when Ethernet is selected as a Frame Type is called 'Etype'. Valid values for Etype ranges from 0x0600 - 0xffff. The default is Etype: 0x0800.

Protocol to Group Mapping Table

| Delete | Frame Type | Value | Group Name |
|--------|------------|---------------|------------|
| Delete | Ethernet | Etype: 0x0800 | |

2. **LLC**: Valid value in this case is comprised of two different sub-values.
 - a. **DSAP**: 1-byte long string (0x00-0xff). The default is DSAP: 0xFF.
 - b. **SSAP**: 1-byte long string (0x00-0xff). The default is SSAP: 0xFF.

Protocol to Group Mapping Table

| Delete | Frame Type | Value | Group Name |
|--------|------------|-----------------------|------------|
| Delete | LLC | DSAP: 0xFF SSAP: 0xFF | |

3. **SNAP**: Valid value in this case also is comprised of two different sub-values.
 - a. **OUI**: OUI (Organizationally Unique Identifier) in the format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff.
 - b. **PID**: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.

Protocol to Group Mapping Table

| Delete | Frame Type | Value | Group Name |
|--------|------------|-----------------------------|------------|
| Delete | SNAP | OUI: 0x00-E0-2B PID: 0x0001 | |

Group Name

A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers (0-9).

Note: special character and underscore () are not allowed in the Group Name field.

Adding a New Group to VLAN mapping entry

Click the **Add New Entry** button to add a new entry in the mapping table. An empty row is added to the table; configure Frame Type, Value and the Group Name as needed. The **Add New Entry** button can be used to undo the addition of a new entry.

Buttons

Save: Click to save changes.

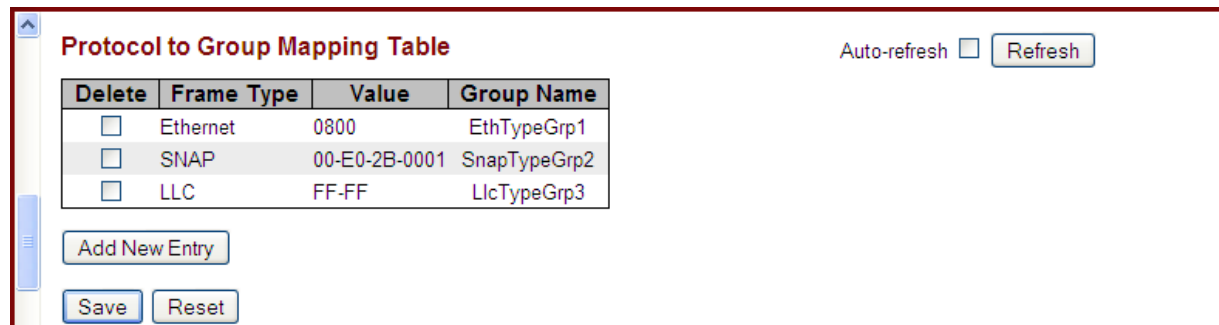
Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Example

The screen below shows three Groups in the mapping table.



The screenshot shows a web interface titled "Protocol to Group Mapping Table". It features a table with four columns: "Delete", "Frame Type", "Value", and "Group Name". The table contains three entries: Ethernet (0800, EthTypeGrp1), SNAP (00-E0-2B-0001, SnapTypeGrp2), and LLC (FF-FF, LlctypeGrp3). Each entry has a checkbox in the "Delete" column. Below the table are buttons for "Add New Entry", "Save", and "Reset". To the right of the table, there is an "Auto-refresh" checkbox and a "Refresh" button.

| Delete | Frame Type | Value | Group Name |
|--------------------------|------------|---------------|--------------|
| <input type="checkbox"/> | Ethernet | 0800 | EthTypeGrp1 |
| <input type="checkbox"/> | SNAP | 00-E0-2B-0001 | SnapTypeGrp2 |
| <input type="checkbox"/> | LLC | FF-FF | LlctypeGrp3 |

Auto-refresh Refresh

Add New Entry

Save Reset

Group to VLAN

The **Configuration > VCL > Protocol-based VLAN > Group to VLAN** menu path lets you configure the S4224 'Group Name to VLAN mapping table' settings. This page lets you map an existing, configured Group Name to a VLAN for the selected switch. At default, the table displays "No Group entries".

Click the **Add New Entry** button to display the entry fields.

The screenshot shows the web interface for the S4224 - Carrier Ethernet Network Interface Device. The page title is "Group Name to VLAN mapping Table". On the left is a navigation menu with options like VCL, MAC-based VLAN, Protocol-based VLAN, and Ethernet Services. The main area contains a table with columns for "Delete", "Group Name", "VLAN ID", and "Port Members" (ports 1-28). Below the table are buttons for "Add New Entry", "Save", and "Reset". There is also an "Auto-refresh" checkbox and a "Refresh" button.

The displayed settings are explained below.

Delete

To delete a Group Name to VLAN map entry, check this box. The entry will be deleted from the S4224 at the next Save.

Group Name

A valid Group Name is a string of up to 16 characters which consists of a combination of alpha (a-z or A-Z) and numeric (0-9) characters; no special characters are allowed. Whichever Group name you try map to a VLAN must be present in the Protocol to Group mapping table (see above) and must not already be used by any other existing mapping entry on this page.

VLAN ID

Indicates the VID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4094.

Port Members

A row of checkboxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members and all boxes are unchecked. At least one Port Member checkbox must be checked.

Add New Entry (Add a New Group to VLAN mapping table)

Click the **Add New Entry** button to add a new entry in the mapping table. An empty row is added to the table; configure the Group Name, VLAN ID and port members as needed. The valid VLAN ID values are **1** to **4094**.

The **'Reset'** button can be used to undo the addition of new entry.

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

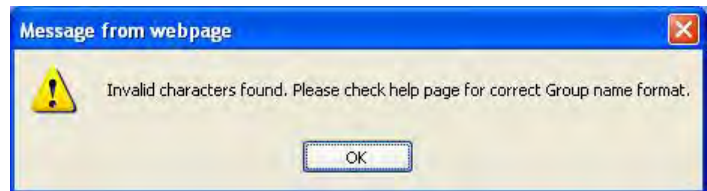
Reset: Click to undo any changes made locally and revert to previously saved values.

Adding a New Group to VLAN mapping entry

The screen below shows three Group Names added to the Group Name to VLAN members table, as configured from the **Configuration - VCL - Group to VLAN** menu path.

| Delete | Group Name | VLAN ID | Port Members | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------------|------------|---------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| <input type="checkbox"/> | VMC2 | 2 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | thirdMC | 2 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | vmc01 | 1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |

If you enter any special characters in the **Group Name** field, the message *'Invalid characters found. Please check help page for correct Group name format'* displays.



Click the **OK** button to clear the webpage message, and then re-enter the Group Name without any special characters (no space characters, underscore characters, dashes, etc.). Click the **Save** button when done.

IP Subnet-based VLAN

IP subnet-based VLAN entries can be configured from the **Configuration > VCL > IP Subnet-based VLAN** menu path. With this method, a VLAN membership is defined by the subnet to which a device's IP address belongs.

This page allows adding, updating and deleting IP subnet to VLAN ID mapping entries and assigning them to different ports.

VLANs are layer 2 constructs, compared with IP subnets which are layer 3 constructs. In an environment employing VLANs, a one-to-one relationship often exists between VLANs and IP subnets, but it is possible to have multiple subnets on one VLAN. VLANs and IP subnets provide independent Layer 2 and Layer 3 constructs that map to each other, and this correspondence helps in network design. Note that this page shows only static entries.

From the default page, click the **Add New Entry** button to display the entry fields.

The screenshot shows the web interface for configuring IP Subnet-based VLAN Membership. The title bar indicates the device is 'S4224 - Carrier Ethernet Network Interface Device'. The left sidebar shows the navigation menu with 'IP Subnet-based VLAN' selected. The main content area is titled 'IP Subnet-based VLAN Membership Configuration' and includes an 'Auto-refresh' checkbox and a 'Refresh' button. Below this is a table with the following structure:

| Delete | IP Address | Mask Length | VLAN ID | Port Members | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------------|------------|-------------|---------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|----|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| <input type="checkbox"/> | 0.0.0.0 | 24 | 1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |

Below the table are buttons for 'Add New Entry', 'Save', and 'Reset'.

The IP subnet-based VLAN entries are explained below.

Delete

To delete an IP subnet-based VLAN entry, check this box and click **Save**. The entry will be deleted from the switch.

IP Address

Sets / shows the IP address. Enter a valid IP address in dotted decimal notation ('x.y.z.w') where x, y, and z are decimal numbers from **0** to **255**. The default IP address of 0.0.0.0 is not valid.

Mask Length

Sets / shows the network mask length. The valid mask length range is **1-32**.

VLAN ID

Sets / shows the VLAN ID. The VLAN ID can be changed for the existing entries.

Port Members

Displays a row of check boxes for each port for each IP subnet-based VLAN entry. To include a port in a IP subnet-based VLAN, check the checkbox. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked. At least one port member must be checked in order to save an entry.

Add New Entry (Add a New IP Subnet-based VLAN)

Click the **Add New Entry** button to add a new IP subnet to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any IP address/mask can be configured for the mapping. Legal values for the VLAN ID are **1** to **4095**.

The IP subnet to VLAN ID mapping entry is enabled when you click on "Save". The button can be used to undo the addition of new mappings. The maximum possible IP subnet to VLAN ID mappings are limited to 128. Note that you can add multiple entries with one Save operation.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh: Check this checkbox to refresh the page automatically every three seconds.

Refresh: Refreshes the displayed table.

Example

In the screen sample below, three IP-subnet based VLANs have been created.

The screenshot shows the web interface for a S4224 Carrier Ethernet Network Interface Device. The main configuration area is titled "IP Subnet-based VLAN Membership Configuration". It features a table with columns for "Delete", "IP Address", "Mask Length", "VLAN ID", and "Port Members" (ports 1-28). Three entries are listed:

| Delete | IP Address | Mask Length | VLAN ID | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
|--------------------------|--------------|-------------|---------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|----|
| <input type="checkbox"/> | 102.201.6.30 | 32 | 1 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | 102.202.6.0 | 24 | 1 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> | 110.10.10.0 | 24 | 1 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |

Below the table are buttons for "Add New Entry", "Save", and "Reset". The "Auto-refresh" checkbox is unchecked, and a "Refresh" button is present.

Each of the three IP-subnet based VLAN has a mix of IP addresses, Mask lengths, VIDs, and port members assigned.

Ethernet Services Configuration

Configuration > Ethernet Services

From the **Configuration > Ethernet Services** menu path you can configure S4224 Ethernet services in terms of ports, bandwidth profiles, EVCs (Ethernet Virtual Circuits) and ECEs (EVC Control Entries).

These pages configure Ethernet Virtual Connections (EVCs) and their configurations using the ECEs. The MEF standards describe services provided to customers at User Network Interfaces (UNIs). Inside provider networks, nodes are connected using Internal Network-to-Network Interfaces (I-NNIs). Connections between service providers are done using External Network-to-Network Interfaces (E-NNIs). An Ethernet Virtual Connection (EVC) is an association of two or more UNIs. Three EVC types are defined:

- E-Line: Point-to-point connection of two UNIs.
- E-LAN: Multipoint-to-multipoint connection of two or more UNIs.
- E-Tree: Rooted-multipoint connection between leaf and root UNIs. Frames are not forwarded between leaf UNIs.

The MEF defines a number of attributes associated with a UNIs and EVCs. These attributes include mappings of customer VLAN IDs to EVCs, ingress bandwidth profiles, processing of L2 control protocols (L2CP) etc.

The S4224 EVC (Ethernet Virtual Connection) commands let you configure S4224 Ethernet services in terms of EVCs and ECEs (EVC Control Entries). Only Provider Bridge based EVCs are supported on the S4224.

The EVC is an association of two or more UNIs that limits the exchange of frames to UNIs in the Ethernet Virtual Connection. The User Network Interface (UNI) is the physical interface or port that is the demarcation between the customer and the service provider / Cable Operator /Carrier / MSO. The UNI is the physical demarcation point between the responsibility of the Service Provider and the responsibility of the Subscriber.

EVC (Ethernet Virtual Connection): An association of two or more UNIs that limits the exchange of frames to UNIs in the EVC. Generally, an EVC allows Ethernet service frames to be exchanged between UNIs that are connected via the same EVC.

ECEs (EVC Control Entries): Unique ECE IDs are automatically assigned to ECEs added. The possible range is from 1 through 128. The ECE ID identifies the ECE.

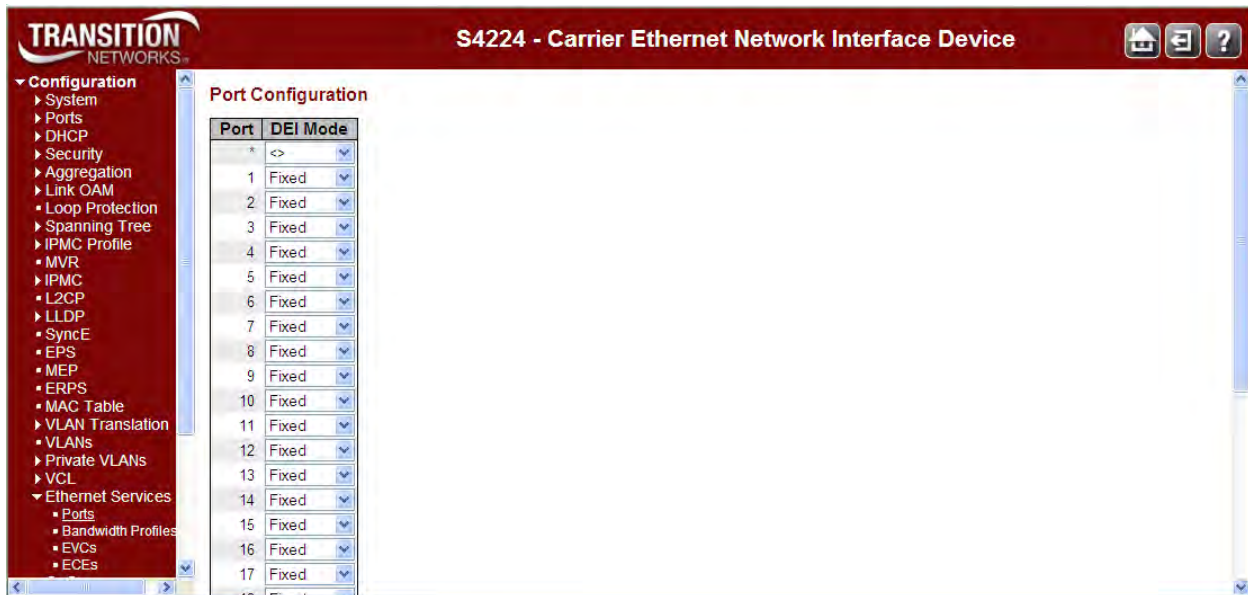
Note: You must set up an EVC before trying to set up a related ECE.

An Ethernet Services configuration procedure will include:

1. EVC Configuration
2. ECE Configuration
3. VLAN Configuration
4. MEP Configuration Procedure
 - a. Down MEP Configuration
 - b. Up MEP Configuration
 - c. Fault Management Configuration
5. EPS Configuration Procedure

Configuration > Ethernet Services > Ports

This page lets you display and change current EVC port configuration settings.



The **Ethernet Services > Ports** configuration settings are explained below.

Port

The logical port for the settings contained in the same row.

DEI Mode

The DEI mode for an NNI port determines whether frames transmitted on the port will have the DEI field in the outer tag marked based on the colour of the frame. The allowed values are:

Coloured: The DEI is 1 for yellow frames and 0 for green frames.

Fixed: The DEI value is determined by ECE rules.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Configuration > Ethernet Services > Bandwidth Profiles

This page displays current EVC ingress bandwidth profile configurations. The policers configured here can be used to limit the traffic received on UNI ports. A policer can limit the bandwidth of received frames. Each policer is located in front of the ingress queue.

The EVC ingress bandwidth profile configurations may be used to limit the traffic received on UNI ports.

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

Bandwidth Profiles Configuration

Start from Policer ID with entries per page.

| Policer ID | State | Type | Policer Mode | Rate Type | CIR (kbps) | CBS (bytes) | EIR (kbps) | EBS (bytes) |
|------------|----------|------|--------------|-----------|------------|-------------|------------|-------------|
| * | <> | <> | <> | <> | 0 | 0 | 0 | 0 |
| 1 | Disabled | MEF | Blind | Data | 0 | 0 | 0 | 0 |
| 2 | Disabled | MEF | Blind | Data | 0 | 0 | 0 | 0 |
| 3 | Disabled | MEF | Blind | Data | 0 | 0 | 0 | 0 |
| 4 | Disabled | MEF | Blind | Data | 0 | 0 | 0 | 0 |
| 5 | Disabled | MEF | Blind | Data | 0 | 0 | 0 | 0 |
| 6 | Disabled | MEF | Blind | Data | 0 | 0 | 0 | 0 |
| 7 | Disabled | MEF | Blind | Data | 0 | 0 | 0 | 0 |
| 8 | Disabled | MEF | Blind | Data | 0 | 0 | 0 | 0 |
| 9 | Disabled | MEF | Blind | Data | 0 | 0 | 0 | 0 |
| 10 | Disabled | MEF | Blind | Data | 0 | 0 | 0 | 0 |
| 11 | Disabled | MEF | Blind | Data | 0 | 0 | 0 | 0 |
| 12 | Disabled | MEF | Blind | Data | 0 | 0 | 0 | 0 |
| 13 | Disabled | MEF | Blind | Data | 0 | 0 | 0 | 0 |
| 14 | Disabled | MEF | Blind | Data | 0 | 0 | 0 | 0 |
| 15 | Disabled | MEF | Blind | Data | 0 | 0 | 0 | 0 |

This page lets you view and configure current EVC ingress bandwidth profile configurations.

Start from Policer ID

The start Policer ID for displaying the table entries. The valid range is **1** - **2048**.

entries per page

The number of entries to be displayed per page. The valid range is **2** - **2048**.

Policer ID

The Policer ID is used to identify one of the 2048 policers.

State

The administrative state of the bandwidth profile. The allowed values are:

- Enabled:** The bandwidth profile enabled.
- Disabled:** The bandwidth profile is disabled.

Type

The policer type of the bandwidth profile. The allowed values are:

- MEF:** MEF ingress bandwidth profile.
- single:** Single bucket policer.

Policer Mode

The colour mode of the bandwidth profile. The allowed values are:

Coupled: Colour-aware mode with coupling enabled.

Aware: Colour-aware mode with coupling disabled.

Blind: Colour-blind mode.

Rate Type

The rate type of the bandwidth profile. The allowed values are:

Data: Specify that this bandwidth profile operates on data rate.

Line: Specify that this bandwidth profile operates on line rate.

CIR

The Committed Information Rate of the bandwidth profile. The valid range is 0 - 10000000 kilobits per second.

CBS

The Committed Burst Size of the bandwidth profile. The valid range is 0 - 100000 bytes.

EIR

The Excess Information Rate for MEF type bandwidth profile. The valid range is 0 - 10000000 kilobit per second.

EBS

The Excess Burst Size for MEF type bandwidth profile. The valid range is 0 - 100000 bytes.

Buttons

Refresh: Refreshes the displayed table starting from the input fields.

|<<: Updates the table, starting with the first entry in the table.

<<: Updates the table, ending at the entry before the first entry currently displayed.

>>: Updates the table, starting with the entry after the last entry currently displayed.

>>|: Updates the table, ending at the last entry in the table.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

BWP Parameters Summary

| Parameter | Valid Range | Default |
|-----------------------|---|----------|
| Policer ID (Readonly) | 1 to 128. Two policer IDs are reserved and cannot be changed. | None |
| State | Enabled or Disabled | Disabled |
| Type | MEF or Single | MEF |
| Policer Mode | Coupled or Aware | Aware |
| Rate Type | Data or Line | Data |
| CIR | 0 to 10000000 kbps | 0 |
| CBS | 0 to 100000 bytes | 0 |
| EIR | 0 to 10000000 kbps | 0 |

For information on factors affecting Carrier Ethernet throughput see the MEF white paper at http://metroethernetforum.org/Assets/White_Papers/Understanding_Carrier_Ethernet_Throughput_-_v14.pdf.

Configuration > Ethernet Services > EVCs

The **Configuration > Ethernet Services > EVCs** menu path displays current EVC configurations. The EVC settings can also be configured here. On this system, only Provider Bridge based EVCs are supported.

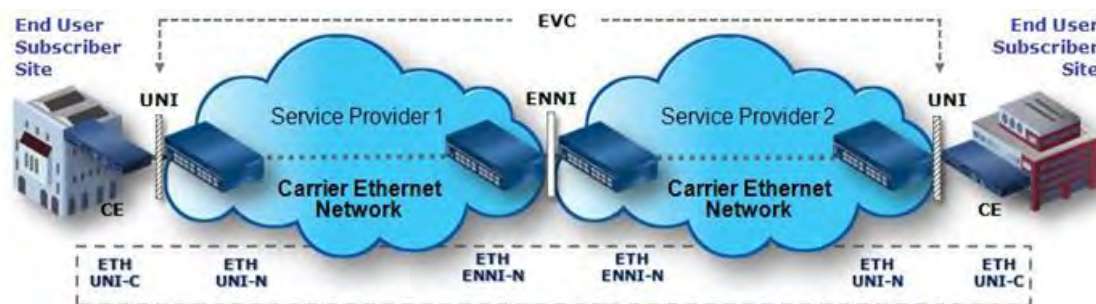


Figure 8. Provider Bridge E-LINE Service

The EVC (Ethernet Virtual Connection) is an association of two or more UNIs that limits the exchange of frames to UNIs in the Ethernet Virtual Connection. The User Network Interface (UNI) is the physical interface or port that is the demarcation between the customer and the service provider/Cable Operator/Carrier/MSO. The UNI is the physical demarcation point between the responsibility of the Service Provider and the responsibility of the Subscriber.

MEF Ethernet Virtual Connection Types

The Metro Ethernet Forum (MEF) specifies these EVC (Ethernet Virtual Connection) types:

E-Line EVC: Point-to-point Service Ethernet Private Line (EPL) allows only one EVC per UNI port, while Ethernet Virtual Private Line (EVPL) allows multiple EVCs per UNI port. The figure below shows a Provider Bridge E-LINE service example.

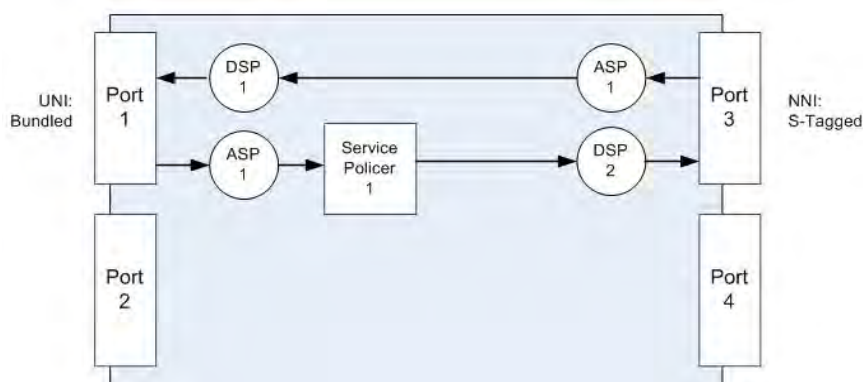


Figure 9. Provider Bridge E-LINE Service

E-LAN EVC: Multipoint Service Ethernet Private LAN (EP-LAN) allows only one EVC per UNI port, while Ethernet Virtual Private LAN (EVP-LAN) allows multiple EVCs per UNI port. This is a bridged service.

E-TREE EVC: Rooted Multipoint Service Ethernet Private Tree (EP-TREE) allows only one EVC per UNI port, while Ethernet Virtual Private Tree (EVP-TREE) allows multiple EVCs per UNI port. This is a bridged service where the root port has access to all the leaf ports, but the leaf ports only have access to the root port.


Configuration Prerequisites

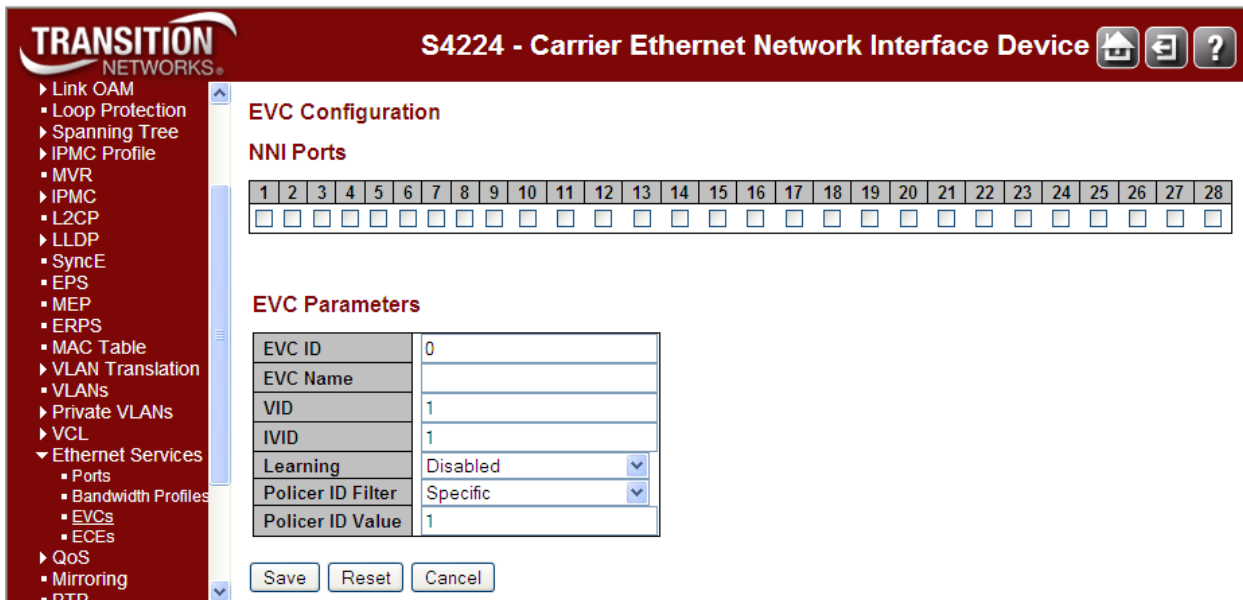
1. E-LINE is supported; you must disable MAC Learning first for E-LINE support.
2. E-LAN is supported; you must remove each VLAN and enable MAC Learning for E-LAN support.

Configuration > Ethernet Services > EVCs

This menu path displays the EVC Control List Configuration table. You can add, edit, and delete EVCs here. Only Provider Bridge based EVCs are supported. The EVC configuration parameters on the default page are shown below.



Click the  button to add a new EVC. The EVC Configuration page displays.



Configure the new EVC's NNI Ports, EVC Parameters, Inner Tag and Outer Tag as explained below.

NNI Ports

The list of Network to Network Interfaces for the EVC.

EVC ID

The EVC ID identifies the EVC. The valid range is from 1 - 4096.

EVC Name

Enter a name for the EVC (optional).

VID

The VLAN ID in the PB (provider bridging) network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The range is 0 - 4095.

IVID

The Internal/classified VLAN ID in the PB (provider bridging) network. The valid range is 1 - 4095.

Learning

The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports. The possible values are:

Enabled: Learning is enabled (MAC addresses are learned).

Disabled: Learning is disabled (MAC addresses are not learned).

Policer ID Filter

The ingress bandwidth profile mode for the EVC. The possible values are:

Specific: The range is from 1 - 256.

Discard: All received frames are discarded for the EVC.

None: None bandwidth profile for the EVC.

| |
|----------|
| Specific |
| Discard |
| None |

Policer ID Value


The value for the Policer ID.


Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Return to the previous page; any changes made locally will be undone.

Click the  modification button to add a new EVC.

Click the  button to edit an existing EVC.

Click the  to delete an existing EVC.

Configuration > Ethernet Services > ECEs

This menu path displays the EVC Control Entries (ECEs). You can add, edit, and delete ECEs here. The default ECE Control List Configuration page is shown below.

| ECE ID | UNI Ports | Ingress Matching | | | | | Direction | Actions | | | | Egress Outer Tag | | | | Conflict | |
|--------|-----------|------------------|-----|-----|-----|------------|-----------|---------|------------|---------------|-----------|------------------|-----|----------------------|-----|----------|-----|
| | | Tag Type | VID | PCP | DEI | Frame Type | | EVC ID | Policer ID | Tag Pop Count | Policy ID | Mode | VID | PCP/DEI Preservation | PCP | | DEI |
| | | | | | | | | | | | | | | | | | |

The ECE Control List Configuration parameters are explained below.

ECE ID

The ECE ID identifies the ECE. Unique ECE IDs are automatically assigned to ECEs added. The valid range is **1 - 4096**.

Ingress Matching

UNI Ports

The list of User Network Interfaces for the ECE.

Tag Type

The tag type for the ECE. The possible values are:

Any: The ECE will match both tagged and untagged frames.

Untagged: The ECE will match untagged frames only.

C-Tagged: The ECE will match custom tagged frames only.

S-Tagged: The ECE will match service tagged frames only.

Tagged: The ECE will match tagged frames only.

VLAN ID Filter

The VLAN ID for the ECE. It only significant if tag type 'Tagged' is selected. The possible values are:

Specific: The range is from **1 - 4094**.

Any: The ECE will match any VLAN ID.

PCP

The PCP value for the ECE. It only significant if tag type 'Tagged' is selected. The possible values are:

Specific: The ECE will match a specific PCP in the range **0 - 7**.

Range: The ECE will match PCP values in the selected range **0-1, 2-3, 4-5, 6-7, 0-3** or **4-7**.

Any: The ECE will match any PCP value.

DEI

The DEI value for the ECE. It only significant if tag type 'Tagged' is selected. The valid values are: **0, 1** or **Any**.

Frame Type

The frame type for the ECE. The possible values are:

Any: The ECE will match any frame type.

IPv4: The ECE will match IPv4 frames only.

IPv6: The ECE will match IPv6 frames only.

| | |
|------------|------|
| Frame Type | Any |
| | IPv4 |
| | IPv6 |

Actions

Direction

The EVCs and ECEs are used to setup flows in one or both directions as determined by the ECE Direction parameter. If the ECE is bidirectional, the ingress rules of the NNI ports will be setup to match the traffic being forwarded to NNI ports. Possible values are:

Both: Bidirectional.

UNI-to-NNI: Unidirectional from UNI to NNI.

NNI-to-UNI: Unidirectional from NNI to UNI.

EVC ID Filter

The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. The possible values are:

None: No EVC ID filter is specified. (EVC ID filter status is "don't-care".)

Specific: If you want to filter a specific EVC ID with this ECE, choose this value. A field for entering a specific value appears.

EVC ID Value

When "Specific" is selected for the EVC ID filter, you can enter a specific value. The allowed value is from **1** through **4096**.

Policer ID Filter

The policer ID filter for matching the ECE. The possible values are:

Specific: If you want to filter a specific policer ID value with this ECE, choose this value. A field for entering a specific value appears.

Discard: All received frames are discarded for the ECE.

None: All received frames are forwarded for the ECE.

EVC: The bandwidth profile for the specified EVC ID is used.

Policer ID Value

When "Specific" is selected for the policer ID filter, you can enter a specific value. The value is from **1** through **2048**.

Tag Pop Count

The ingress tag pop count for the ECE. The valid range is **0** - **2**.

Policy ID

The ACL Policy ID for the ECE. The valid range is **0** - **63**.

Egress Outer Tag

Mode

The outer tag for nni-to-uni direction for the ECE. The possible values are:

Enable: Enable outer tag for nni-to-uni direction for the ECE.

Disable: Disable outer tag for nni-to-uni direction for the ECE.

VLAN ID

The EVC outer tag VID (VLAN ID) for UNI ports. The valid range is **0** - **4095**.

PCP Mode

The outer tag PCP mode for the ECE. The possible values are:

Classified: The outer tag PCP Mode is classified.

Fixed: The outer tag PCP Mode is fixed.

Mapped: The outer tag PCP Mode is based on mapped (QOS, DP).

PCP

The PCP value (**0-7**).

DEI Mode

The outer tag DEI mode for the ECE. The possible values are:

Classified: The outer tag DEI mode is classified.

Fixed: The outer tag DEI mode is fixed.

Drop Precedence: The outer tag DEI mode is drop precedence.

DEI


The DEI value (**0** or **1**).

Conflict

Indicates the hardware status of the specific ECE. If **Yes**, the specific ECE is not applied to the hardware due to hardware limitations.

Modification Buttons

You can modify each ECE (EVC Control Entry) in the table using the following buttons:


: Inserts a new ECE before the current row.

: Edits the ECE row.

: Moves the ECE up the list.

: Moves the ECE down the list.

: Deletes the ECE.

: The lowest plus sign adds a new entry at the bottom of the ECE listings.

Buttons

Auto-refresh: Check the checkbox to refresh the page automatically every three seconds.

Refresh: Click to refresh the page.

Remove All: Click to remove all ECEs. At the Confirm prompt, click the **OK** button to proceed or click the Cancel button to cancel.

ECE Configuration Page

When you click a plus (+) sign to add a new entry to the ECE listings, the **ECE Configuration** page displays.

Configure the new ECE’s UNI Ports, UNI Matching, Actions, MAC Parameters, IPv4, IPv6, NNI Outer Tag, and/or NNI Inner Tag parameters as explained above. **Note:** the set of parameters displayed here depend on the **Frame Type** selection at the **UNI Matching** section.

The **ECE Configuration** page parameters are explained below.

UNI Ports

The list of User Network Interfaces for the ECE. Check or uncheck one or more of the checkboxes.

Ingress Matching

Tag Type

The tag type for matching the ECE. The possible values are:

Any: The ECE will match both tagged and untagged frames.

Untagged: The ECE will match untagged frames only.

C-Tagged: The ECE will match custom tagged frames only.

S-Tagged: The ECE will match service tagged frames only.

Tagged: The ECE will match tagged frames only.

Inner Tag Type

The tag type for matching the ECE. The possible values are:

Any: The ECE will match both tagged and untagged frames.

Untagged: The ECE will match untagged frames only.

C-Tagged: The ECE will match custom tagged frames only.

S-Tagged: The ECE will match service tagged frames only.

Tagged: The ECE will match tagged frames only.

VLAN ID Filter

The VLAN ID filter for matching the ECE. It only significant if tag type 'Tagged' is selected. The possible values are:

Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)

Specific: If you want to filter a specific VLAN ID value with this ECE, choose this value. A field for entering a specific value appears.

Range: If you want to filter a specific VLAN ID range filter with this ECE, choose this value. A field for entering a range appears.

VLAN ID Value

When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is 0 - 4095.

VLAN ID Range

When "Range" is selected for the VLAN ID filter, you can enter a specific range. The range needs to be based on a bit mask. For example:\n160 (10100000 in binary) can go to\n161 (10100001)\n163 (10100011)\n167 (10100111)\n175 (10101111) or\n191 (10111111).

Ingress Matching

| | | |
|----------------|--------|-----|
| Tag Type | Tagged | ▼ |
| VLAN ID Filter | Range | ▼ |
| VLAN ID Range | 10 | -11 |

PCP

The PCP value for matching the ECE. It only significant if tag type 'Tagged' is selected. Valid values are:

Any: The ECE will match any PCP value.

Specific: The ECE will match a specific PCP in the range 0 through 7.

Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.

DEI

The DEI value for matching the ECE. It only significant if tag type 'Tagged' is selected. The allowed value is: 0, 1 or Any.

The inner tag type for matching the ECE. The possible values are:

Any: The ECE will match both tagged and untagged frames.

Tagged: The ECE will match tagged frames only.

C-Tagged: The ECE will match custom tagged frames only.

S-Tagged: The ECE will match service tagged frames only.

Untagged: The ECE will match untagged frames only.

The inner VLAN ID filter for matching the ECE. It only significant if tag type 'Tagged' is selected.

The possible values are:

Any: No inner VLAN ID filter is specified. (Inner VLAN ID filter status is "don't-care".)

Specific: If you want to filter a specific inner VLAN ID value with this ECE, choose this value. A field for entering a specific value appears.

Range: If you want to filter a specific inner VLAN ID range filter with this ECE, choose this value. A field for entering a range appears.

When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is 0 - 4095.

When "Range" is selected for the VLAN ID filter, you can enter a specific range. The allowed range is 0 - 4095.

The inner PCP value for matching the ECE. It only significant if inner tag type 'Tagged' is selected. The possible values are:

Any: The ECE will match any PCP value.

Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.

Specific: The ECE will match a specific PCP in the range 0 through 7.

The inner DEI value for matching the ECE. It only significant if inner tag type 'Tagged' is selected. The allowed value is: 0, 1 or Any.

Inner VLAN ID Filter

The inner VLAN ID filter for matching the ECE. It only significant if tag type 'Tagged' is selected. The possible values are:

Any: No inner VLAN ID filter is specified. (Inner VLAN ID filter status is "don't-care".)

Specific: If you want to filter a specific inner VLAN ID value with this ECE, choose this value. A field for entering a specific value appears.

Range: If you want to filter a specific inner VLAN ID range filter with this ECE, choose this value. A field for entering a range appears.

Inner VLAN ID Value

When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is from 0 through 4095.

Inner Tag VLAN ID Range

When "Range" is selected for the VLAN ID filter, you can enter a specific range. The allowed range is 0 - 4095.

Inner PCP

The inner PCP value for matching the ECE. It is only significant if inner tag type 'Tagged' is selected. The possible values are: **Any** (the ECE will match any PCP value), a specific PCP in the range 0 through 7, or 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.

Inner DEI

The inner DEI value for matching the ECE. It only significant if inner tag type 'Tagged' is selected. The allowed value is: 0, 1 or **Any**.

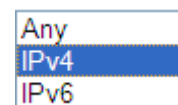
Frame Type

The frame type for the ECE. The possible values are:

Any: The ECE will match any frame type.

IPv4: The ECE will match IPv4 frames only. Additional parameters display when selected.

IPv6: The ECE will match IPv6 frames only. Additional parameters display when selected.



DSCP Filter

The DSCP filter for matching the ECE. The possible values are:

Any: No DSCP filter is specified. (DSCP filter status is "don't-care".)

Specific: If you want to filter a specific DSCP value with this ECE, choose this value. A field for entering a specific value appears.

Range: If you want to filter a specific DSCP range filter with this ECE, choose this value. A field for entering a range appears.

DSCP Value

When "Specific" is selected for the DSCP filter, you can enter a specific value. The allowed value is from **0** through **63**.

DSCP Range

When "Range" is selected for the DSCP filter, you can enter a specific range. The allowed range is from **0** through **63**.

MAC Parameters

The source/destination MAC address for matching the ECE. It depends on by the port address mode; when port address mode is set to 'Source' then the field is used for source MAC address. Similarly when port address mode is set to 'Destination' then the field is used for destination MAC address.

DMAC Filter

The possible values are:

Any: No destination MAC address is specified.

Unicast: Frame must be unicast.

Multicast: Frame must be multicast.

Broadcast: Frame must be broadcast.

specific: Lets you enter a specific DMAC Value.

MAC Parameters

| | |
|-------------|-----------|
| DMAC Filter | Specific |
| DMAC Value | Any |
| | Unicast |
| | Multicast |
| | Broadcast |
| | Specific |

DMAC Value

The Destination MAC address (e.g., 00-00-00-00-00-01). When "Specific" is selected for the DMAC filter, you can enter a specific value. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit).

Actions

Direction

The EVCs and ECEs are used to setup flows in one or both directions as determined by the ECE Direction parameter. If the ECE is bidirectional, the ingress rules of the NNI ports will be setup to match the traffic being forwarded to NNI ports. The possible values are:

Both: Bidirectional.

UNI-to-NNI: Unidirectional from UNI to NNI.

NNI-to-UNI: Unidirectional from NNI to UNI.

Actions

| | |
|-------------------|----------|
| Direction | Both |
| EVC ID Filter | Specific |
| EVC ID Value | 1 |
| Policer ID Filter | None |
| Tag Pop Count | 0 |
| Policy ID | 0 |

EVC ID Filter

The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. The possible values are:

None: No EVC ID filter is specified. (EVC ID filter status is "don't-care".)

specific: If you want to filter a specific EVC ID with this ECE, choose this value. A field for entering a specific value displays.

EVC ID Value

When "Specific" is selected for the EVC ID filter, you can enter a specific value. The allowed value is from **1** through **256**.

The policer ID filter for matching the ECE. The possible values are:

specific: If you want to filter a specific policer ID value with this ECE, choose this value. A field

for entering a specific value displays.

Discard: All received frames are discarded for the ECE.

None: All received frames are forwarded for the ECE.

EVC: The bandwidth profile for the specified EVC ID is used.

When "Specific" is selected for the policer ID filter, you can enter a specific value. Valid values are **1 - 256**.

Policer ID Filter

The policer ID filter for matching the ECE. The possible values are:

Specific: If you want to filter a specific policer ID value with this ECE, choose this value. A field for entering a specific value appears.

Discard: All received frames are discarded for the ECE.

None: All received frames are forwarded for the ECE.

EVC: The bandwidth profile for the specified EVC ID is used.

Policer ID Value

When "Specific" is selected for the policer ID filter, you can enter a specific value (**1 - 256**).

Tag Pop Count

The ingress tag pop count for the ECE. The allowed range is from **0 - 2**.

Policy ID

The ACL Policy ID for the ECE for matching ACL rules. The allowed range is from **0 - 63**.

The traffic class for the ECE. The valid range is **0 - 8** or **disabled**.

Egress Outer Tag

Mode

The outer tag for nni-to-uni direction for the ECE.

Shows **Disabled** (grayed out) unless the **Direction** is set to **NNI-to-UNI** in the **Actions** section. The possible values are:

Enabled: Enable outer tag for nni-to-uni direction for the ECE.

Disabled: Disable outer tag for nni-to-uni direction for the ECE.

Egress Outer Tag

| | |
|----------------------|--|
| Mode | Enabled <input type="button" value="v"/> |
| VLAN ID | 1 <input type="button" value="v"/> |
| PCP/DEI Preservation | Fixed <input type="button" value="v"/> |
| PCP | 0 <input type="button" value="v"/> |
| DEI | 0 <input type="button" value="v"/> |

VLAN ID

The EVC outer tag VID for UNI ports. The allowed value is from **0 - 4095**.

PCP/DEI Preservation

The outer tag PCP and DEI preservation for the ECE. The possible values are:

Preserved: The outer tag PCP and DEI is preserved.

Fixed: The outer tag PCP and DEI is fixed.

PCP

The outer tag PCP value for the ECE. The valid range is **0 - 7**.

DEI

The outer tag DEI value for the ECE. The allowed value is **0** or **1**.

Egress Inner Tag

Type

The inner type for the ECE determines whether an inner tag is inserted in frames forwarded to NNI ports.

Possible values are:

None: An inner tag is not inserted.

C-tag: An inner C-tag is inserted.

S-tag: An inner S-tag is inserted.

S-custom-tag: An inner tag is inserted and the tag type is determined by the VLAN port configuration of the NNI.

Egress Inner Tag

| | |
|----------------------|-------|
| Type | None |
| VLAN ID | 1 |
| PCP/DEI Preservation | Fixed |
| PCP | 0 |
| DEI | 0 |

VLAN ID

The inner tag VLAN ID for the ECE. The allowed range is **0** - **4095**.

PCP/DEI Preservation

The outer tag PCP and DEI preservation for the ECE. The possible values are:

Preserved: The outer tag PCP and DEI is preserved.

Fixed: The outer tag PCP and DEI is fixed.

PCP

The inner tag PCP value for the ECE. The allowed range is **0** - **7**.

DEI

The inner tag DEI value for the ECE. The allowed values are **0** or **1**.

Buttons


Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.


Cancel: Return to the previous page; any changes made locally will be undone.

Modification Buttons


You can modify each ECE (EVC Control Entry) in the table using the following buttons:


: Inserts a new ECE before the current row.

: Edits the ECE row.

: Moves the ECE up the list.

: Moves the ECE down the list.

: Displays the webpage message “Do you want to delete this entry?” Click **OK** to delete the ECE.

: The lowest plus sign adds a new entry at the bottom of the ECE listings.

Ethernet Services Application Example

E-Line services are typically used to replace TDM private lines and use two dedicated UNI ports. It is the most common type of Ethernet Service type. The transport-oriented Ethernet Private Line service provides an interconnection between switching or routing equipment in a private data network. This is an ideal service for a Subscriber that needs to manage its own network infrastructure and the Service Provider is providing point-to-point services between two designated UNIs at an agreed upon UNI port speed. An Ethernet Virtual Private Line service can be used to map one or more CE-VLAN IDs to an EVC if multiple services are required.

An EVPL service is commonly used for connecting Subscriber hub and branch locations.

An example EPL service may be configured on two S4224s with the GUI or CLI:

Remove existing VLANs and change switchport interface mode to hybrid, default port-type will be C-Port:

```
#conf t
(config)#no interface vlan 2-4094
(config)#interface GigabitEthernet 1/2-4 2.5GigabitEthernet 1/1-2
(config-if)#switchport mode hybrid
(config-if)#exit
```

Establish the S-Port interface on GigabitEthernet port 1/3:

```
(config)#interface GigabitEthernet 1/3
(config-if)#switchport hybrid port-type s-port
(config-if)#exit
```

Define EVC with VID 11, IVID 1001 and NNI port as GigabitEthernet port 1/3. Configure Ethernet Control Entry 1 for EVC 1 with the UNI port as GigabitEthernet Port 1/2:

```
(config)#evc 1 vid 11 ivid 1001 interface GigabitEthernet 1/3
(config)#evc ece 1 interface GigabitEthernet 1/2 evc 1
```

The screenshot displays the web interface for an S4224 Carrier Ethernet Network Interface Device. The left sidebar contains a navigation menu with options like EPS, MEP, ERPS, MAC Table, VLAN Translation, VLANs, Private VLANs, VCL, Ethernet Services, Performance Monitor, QoS, Mirroring, PTP, GVRP, Service Activation, DDMI, UDLD, Monitor, and Diagnostics. The main content area is titled 'EVC Configuration' and includes the following sections:

- NNI Ports:** A grid of 28 checkboxes representing ports 1 through 28. Ports 3 and 4 are checked.
- EVC Parameters:** A table with the following values:

| | |
|-------------------|----------|
| EVC ID | 2 |
| EVC Name | |
| VID | 10 |
| IVID | 1 |
| Learning | Enabled |
| Policer ID Filter | Specific |
| Policer ID Value | 1 |

At the bottom of the configuration area, there are 'Save', 'Reset', and 'Cancel' buttons.

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

ECE Configuration

UNI Ports

| | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Ingress Matching

| | |
|----------------|-----|
| Tag Type | Any |
| Inner Tag Type | Any |
| Frame Type | Any |

Actions

| | |
|-------------------|----------|
| Direction | Both |
| EVC ID Filter | Specific |
| EVC ID Value | 1 |
| Policer ID Filter | Specific |
| Policer ID Value | 1 |
| Tag Pop Count | 0 |
| Policy ID | 0 |

MAC Parameters

| | |
|-------------|-----|
| DMAC Filter | Any |
|-------------|-----|

Egress Outer Tag

| | |
|----------------------|----------|
| Mode | Disabled |
| VLAN ID | 1 |
| PCP/DEI Preservation | Fixed |
| PCP | 0 |
| DEI | 0 |

Egress Inner Tag

| | |
|----------------------|-------|
| Type | None |
| VLAN ID | 1 |
| PCP/DEI Preservation | Fixed |
| PCP | 0 |
| DEI | 0 |

Save Reset Cancel

Subscribers with multiple sites that need to be on the same LAN would configure an E-LAN Service. In an Ethernet Private LAN service CE-VLAN ID and Class of Service preservation applies so typically no coordination with a Service Provider is needed. One or more Bandwidth Profile flows can be based on a CoS identifier. An EP-LAN Service is configured for all-to-one bundling and therefore services are port based with all CE-VLAN IDs mapping to a single EVC. In an Ethernet Virtual Private LAN service, the multipoint-to-multipoint EVC service has service multiplexing capability to support more than one EVC.

An example EP-LAN service may be configured on two S4224s with the GUI or CLI. This service features a single EVC with one UNI port on device 1 and two UNI ports on device 2 using VID 11.

Device 1:

```
#conf t
(config)#no int vlan 2-4094
(config)#int Gi 1/2-4 2.5Gi 1/1-2
(config-if)#switchport mode hybrid
(config-if)#exit
(config)#int 2.5GigabitEthernet 1/2
(config-if)#switchport hybrid port-type s-port
(config-if)#exit
(config)#evc 3 vid 11 ivid 1001 interface 2.5GigabitEthernet 1/2 learning
```

Configure the EVC Ethernet Control Entry 1 for UNI port GigabitEthernet 1/2. All tagged frames are matched in EVC 3:

```
(config)#evc ece 1 interface GigabitEthernet 1/2 outer-tag match type tagged evc 3
```

On device 2 remove the VLANs and identify the s-port as on device 1. Then configure EVC 3 for ports GigabitEthernet 1/2 and 1/3:

```
(config)#evc 3 vid 11 ivid 1001 interface 2.5GigabitEthernet 1/2 learning
(config)#evc ece 1 interface GigabitEthernet 1/2,3 outer-tag match type tagged evc 3
```

Note: MAC learning is enabled for EVCs with more than two ports so that source addresses are learned for frames matching the EVC.

An Ethernet Private Tree service can give subscribers the opportunity to interconnect multiple sites to provide services other than those resembling a LAN. This type of service is known as a rooted multi-point service because the root is able to communicate with the leaves but the leaves are not able to communicate. CE-VLAN tag preservation and tunneling of L2CP frames are features of an EP-Tree service where each UNI associated by an EVC has one EVC. An Ethernet Virtual Private Tree service can be used to interconnect participating UNIs to a well-defined access, or root point. For example if a customer has an EVP-LAN service providing data connectivity between four UNIs while using an EVP-Tree service to provide video broadcasts from a video hub location. In an EVP-Tree service, at least one CE-VLAN ID is mapped to each EVC.

An E-Access service type can be used to create a broad range of Ethernet access services. An Access EPL service can provide a high degree of transparency for frames, similar to an EPL service such that the frames header and payload upon ingress at the UNI is delivered unchanged to the ENNI with the addition of an S-VLAN tag. The S-VLAN tag is removed upon delivery to the UNI from the ENNI. A Service Provider can use an Access EPL service from an Access Provider to deliver port-based Ethernet services. At the SP ENNI a unique SVLAN ID per Access EPL maps to a single OVC, or Operator Virtual Connection End Point. The Service Provider and Access Provider coordinate the value of the S-VLAN ID at the ENNI. There is no need for coordination between the Subscriber and Service Provider because all Service Frames at the UNI are mapped to a single OVC End Point. Alternatively, an Access EVPL can support multiple service instances including a mix of Access and EVC services.

An example Access **EVPL** service with two OVCs is provisioned with two OVC End Points on device 1. OVC EP1 will pass single tag frames with CE-VLAN ID 1 and OVC EP2 will pass single tag frames with CE-VLAN ID 2 on UNI Port 2 ingress. Device 2 also has two OVC End Points. OVC EP3 is mapped on device 2 and double tagged frames with S-VLAN ID 11 and CE-VLAN ID 1 will be seen on egress ENNI port 2.5GigabitEthernet 1/2. OVC EP 4 is mapped to device 2 and will have double tagged frames with S-VLAN ID 2 and CE-VLAN ID 2 on the same egress ENNI.

Device 1:

```
#conf t
(config)#no int vlan 2-4094
(config)#int Gi 1/2-4 2.5Gi 1/1-2
(config-if)#switchport mode hybrid
(config-if)#exit
(config)#int 2.5GigabitEthernet 1/2
(config-if)#switchport hybrid port-type s-port
(config-if)#exit
(config)#evc 1 vid 11 ivid 1001 interface 2.5GigabitEthernet 1/2
(config)#evc 2 vid 22 ivid 1002 interface 2.5GigabitEthernet 1/2
```

TRANSITION NETWORKS

S4224 - Carrier Ethernet Network Interface Device

ECE Configuration

UNI Ports

| | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Ingress Matching

| | |
|----------------|--------|
| Tag Type | Tagged |
| VLAN ID Filter | Range |
| VLAN ID Range | 0 1 |
| PCP | Any |
| DEI | Any |
| Inner Tag Type | Any |
| Frame Type | Any |

Actions

| | |
|-------------------|----------|
| Direction | Both |
| EVC ID Filter | Specific |
| EVC ID Value | 1 |
| Policer ID Filter | Specific |
| Policer ID Value | 1 |
| Tag Pop Count | 0 |
| Policy ID | 0 |

MAC Parameters

| | |
|-------------|-----|
| DMAC Filter | Any |
|-------------|-----|

Egress Outer Tag

| | |
|----------------------|----------|
| Mode | Disabled |
| VLAN ID | 1 |
| PCP/DEI Preservation | Fixed |
| PCP | 5 |
| DEI | 0 |

Egress Inner Tag

| | |
|----------------------|-------|
| Type | None |
| VLAN ID | 1 |
| PCP/DEI Preservation | Fixed |
| PCP | 0 |
| DEI | 0 |

Save Reset Cancel

Configure EVC ECE 1 for UNI port GigabitEthernet 1/2. Tagged frames are matched with vid 0-1 with PCP 5 in OVC 5:

```
(config)#evc ece 1 interface GigabitEthernet 1/2 outer-tag match type tagged vid 0-1
add pcp 5 evc 3
```

Configure EVC ECE 2 also for UNI port GigabitEthernet 1/2. Untagged frames are matched with PCP 5 in OVC 5:

```
(config)#evc ece 2 interface GigabitEthernet 1/2 outer-tag match type untagged add
pcp 5 evc 3
```

Configure the final EVC ECE 3 also for UNI port GigabitEthernet 1/2. Untagged frames are matched with PCP 5 in OVC 6:

```
(config)#evc ece 3 interface GigabitEthernet 1/2 outer-tag match type tagged add pcp
1 evc 4
```

Device 2:

```
#conf t
(config)#no int vlan 2-4094
(config)#int Gi 1/2-4 2.5Gi 1/1-2
(config-if)#switchport mode hybrid
(config-if)#exit
(config)#int 1/2 2.5GigabitEthernet 1/2
(config-if)#switchport hybrid port-type s-port
(config-if)#switchport hybrid allowed vlan 11,22
```

Configure both ports GigabitEthernet 1/2 and 2.5GigabitEthernet 1/2 as S-ports. Allow both S-VLAN IDs 11 and 22 on these ports. In this configuration, OVC 5 is represented by OVC End Points 1 and 2 and OVC6 by OVC End Points 3 and 4. In this way two Operator Virtual Connection services can exist on each ENNI.

| ECE ID | UNI Ports | Ingress Matching | | | | | Direction | Actions | | | | Egress Outer Tag | | | | Conflict | |
|--------|-----------|------------------|-------|-----|-----|------------|-----------|---------|------------|---------------|-----------|------------------|-----|----------------------|-----|----------|-----|
| | | Tag Type | VID | PCP | DEI | Frame Type | | EVC ID | Policer ID | Tag Pop Count | Policy ID | Mode | VID | PCP/DEI Preservation | PCP | | DEI |
| 1 | 2 | Tagged | 0 - 1 | Any | Any | Any | Both | 1 | 1 | 0 | 0 | Disabled | 1 | Fixed | 0 | 0 | No |
| 2 | 2 | Untagged | - | - | - | Any | Both | 3 | 1 | 0 | 0 | Disabled | 1 | Fixed | 0 | 0 | No |
| 3 | 2 | Tagged | Any | Any | Any | Any | Both | 1 | 1 | 0 | 0 | Disabled | 1 | Fixed | 0 | 0 | No |

Performance Monitor Configuration

S4224 Performance Monitor configuration is performed from the **Configuration > Performance Monitor** menu path. Here you can set PM Session and Storage configuration and Transfer Mode parameters.

PM Session and Storage Configuration

Configure Perf Mon PM Session and storage from **Configuration > Performance Monitor > Configuration**.

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

PM Session and Storage Configuration

| Type | Enable Session | Enable Storage | Measurement Interval(mins) |
|---------------------------|--------------------------|--------------------------|----------------------------|
| Loss Measurement | <input type="checkbox"/> | <input type="checkbox"/> | 15 |
| Delay Measurement | <input type="checkbox"/> | <input type="checkbox"/> | 15 |
| Delay Measurement Binning | | <input type="checkbox"/> | |
| EVC | <input type="checkbox"/> | <input type="checkbox"/> | 15 |

Save Reset

The parameters are described below.

Type

The data type of performance monitor.

Enable Session

Enable or disable the performance monitor session.

Enable Storage

Enable or disable the performance monitor storage.

Measurement Interval(mins)

The measurement interval for the performance monitor.

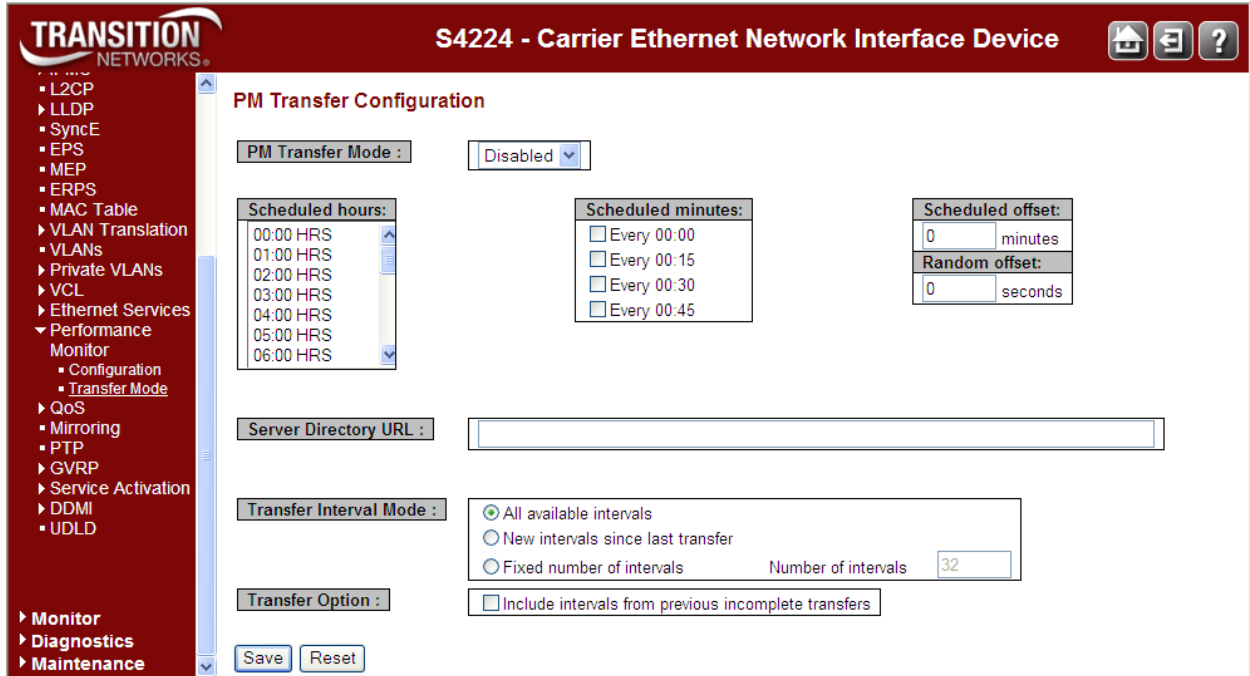
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

PM Transfer Configuration

Configure Perf Mon(PM) transfers from **Configuration > Performance Monitor > Transfer Mode**.



The parameters are described below.

Type

The data type of performance monitor.

PM Transfer Mode

Configure the operation mode per system. Possible modes are:

Enabled: Enable PM Transfer Mode.

Disabled: Disable PM Transfer Mode.

Scheduled Hours

Here you can select one or more of the 24 hours in a day when PM data transfer will occur.

- 00:00
- 01:00
- 02:00
- 03:00
- 04:00
- : : :
- 20:00
- 21:00
- 22:00
- 23:00

The default is none selected.

Scheduled Minutes

Select one or more of the four 15 minute parts of an hour when PM data transfer will occur.

00:00

00:15

00:30

00:45

Default is none selected.

Scheduled Offset

It is possible to configure a fixed offset that is added to the scheduled transfer time.

The range is 0-15 minutes. The default is 0 min.

The sum of Scheduled Fixed Offset and Scheduled Random Offset must not exceed 15 min.

Random Offset

It is possible to configure a random offset that is added to the scheduled transfer time.

The offset added to the scheduled transfer time must be a random value in the range 0-Scheduled Offset.

The range is 0-900 seconds. The default is 0 sec.

The sum of Scheduled Offset and Random Offset must not exceed 15 min.

Server Directory URL

Here you can configure the full URL of the server and the corresponding directory (if any) for uploading.

The supported protocols are HTTP and TFTP.

To enable **HTTP** by entering `http://` followed by the domain name or IP address.

To enable **TFTP** by entering `tftp://` followed by the domain name or IP address.

Transfer Interval Mode

There are three supported interval modes.

All available intervals: To enable transfer of all completed Measurement Intervals.

New intervals since last transfer: To enable transfer of only completed Measurement Intervals since last transfer.

Fixed number of intervals: To enable transfer of all completed Measurement Intervals up to the configured number.

Number of intervals

With **Fixed number of intervals** selected, this value is used to determine the number of intervals to send. The range is 1 to 96 Intervals.

Transfer Option

When this option is checked, PM data transfer will include the suspended (incomplete) transmission.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

QoS Configuration

S4224 QoS Configuration is performed from the **Configuration > QOS** menu path. Quality of Service (QoS) is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required QoS becomes the secret to a successful end-to-end business solution. QoS provides a set of techniques to manage network resources to achieve this success.

Bandwidth Profiling

MEF 10.2 defines 'a bandwidth profile' as "a method of characterizing Service Frames for the purpose of rate enforcement or policing." A sample bandwidth profile use case for a provider dropping a port at an enterprise customer for triple-play services (video, voice and data). The provider may have a Service level agreement with a customer for 5M for video, 3M for voice and 4M for data service, but the overall service cannot exceed 7M for that subscriber.

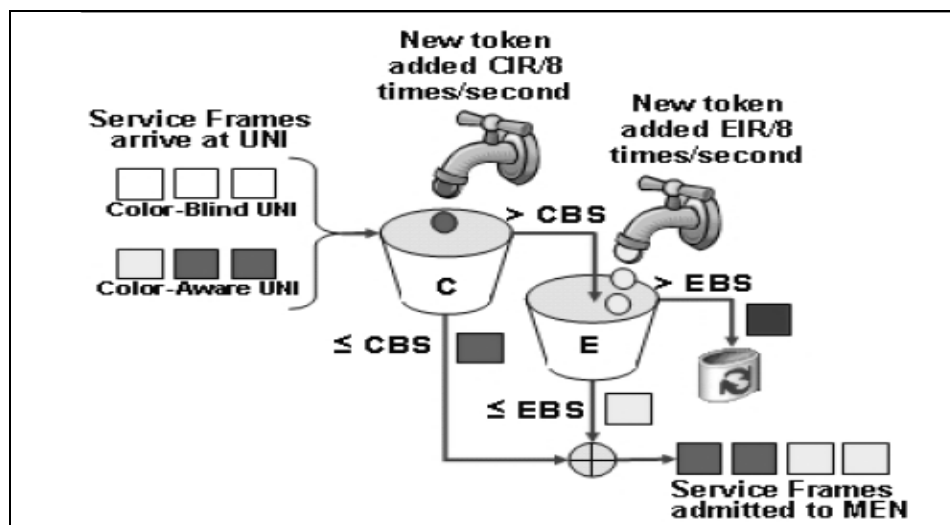


Figure 10. Color Aware Token Bucket Profile for Bandwidth Profiling

The S4224 device supports bandwidth profiling per MEF 10.2, section 7.11 at three levels:

1. Ingress bandwidth profile per UNI (port),
2. Ingress bandwidth profile per EVC (VLAN) per UNI, and
3. Ingress bandwidth profile per Cos per EVC per UNI

For options 2 and 3, the S4224 can provide an overall UNI bandwidth profile as well.

Configuration is performed from the **Ethernet Services > Bandwidth Policies** menu path. The types are 1. MEF (not a true leaky bucket), or 2. Single (no EIR support). These are supported by MEF 10.2. This is technically not a leaky bucket but it is referred to as a token bucket profile in MEF10.2 (which does not mention a leaky bucket). This profile is only used for the EVC configuration. The bucket is essentially not "leaking", the frames may be marked as yellow so they do not actually leave the bucket profile. It also is important to distinguish between the two types of traffic conditioning. The type in the QoS section is a port based single-rate conditioner and the MEF policer is a two-rate three color marker conditioner (trTCM).

The figure below illustrates a provider's SLA with a customer for 5M video / 3M voice / 4M data service where the overall service cannot exceed 7M for that subscriber.

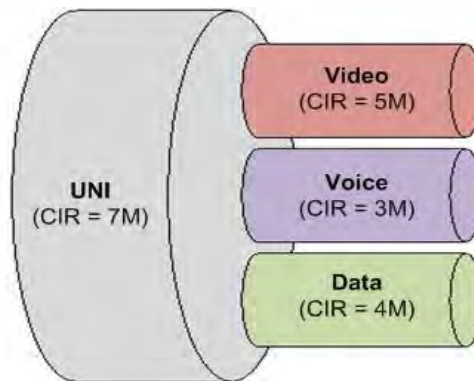


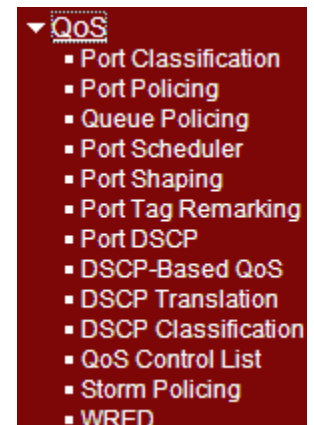
Figure 11. Example SLA for Bandwidth profiling

QoS Configuration Sub-menus

S4224 QoS configuration sub-menus include Port Classification, Port Policing, Queue Policing, Port Scheduler, Port Shaping, Port Tag Remarking, Port DSCP, DSCP-Based QoS, DSCP Translation, DSCP Classification, QoS Control List, and Storm Policing configuration.

Note that the functions configured at **Configuration > QoS** are monitored at the **Monitor > Ports** menu path.

Each of these QoS configuration sub-menus is explained below.



Port Classification

The **Configuration > QoS > Port Classification** menu path displays the QoS Ingress Port Classification page. This page lets you configure the basic QoS Ingress Classification settings for all switch ports.

| Port | CoS | DPL | PCP | DEI | Tag Class. | DSCP Based |
|------|-----|-----|-----|-----|------------|--------------------------|
| * | <> | <> | <> | <> | | <input type="checkbox"/> |
| 1 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 2 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 3 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 4 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 5 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 6 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 7 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 8 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 9 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 10 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 11 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 12 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 13 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 14 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 15 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 16 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 17 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 18 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 19 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 20 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 21 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 22 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 23 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 24 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 25 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 26 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 27 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |
| 28 | 0 | 1 | 0 | 0 | Disabled | <input type="checkbox"/> |

The displayed Port Classification settings are explained below.

Port

The port number for which the configuration below applies.

CoS

Controls the default class of service (**0-7**). All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of **0** (zero) has the lowest priority (default). If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS.

The classified CoS can be overruled by a QCL entry.

Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.

DPL

Controls the default drop precedence level (DPL **0-3**). All frames are classified to a drop precedence level. The default is DPL = **1**.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL.

The classified DPL can be overruled by a QCL entry.

PCP

Controls the default PCP value. All frames are classified to a PCP value of **0-7**. The default is **0**.

If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.

DEI

Controls the default DEI value. All frames are classified to a DEI value of **0** or **1**. The default is **0**.

If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.

Tag Class.

Shows the classification mode for tagged frames on this port.

Disabled: Use default CoS and DPL for tagged frames. This is the default.

Enabled: Use mapped versions of PCP and DEI for tagged frames.

Click on the linked mode (Enabled or Disabled) to configure the mode and/or mapping. The “QoS Ingress Port Classification” page displays.

Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.

DSCP Based

Check the checkbox to enable DSCP Based QoS Ingress Port Classification. The default is unchecked (disabled)

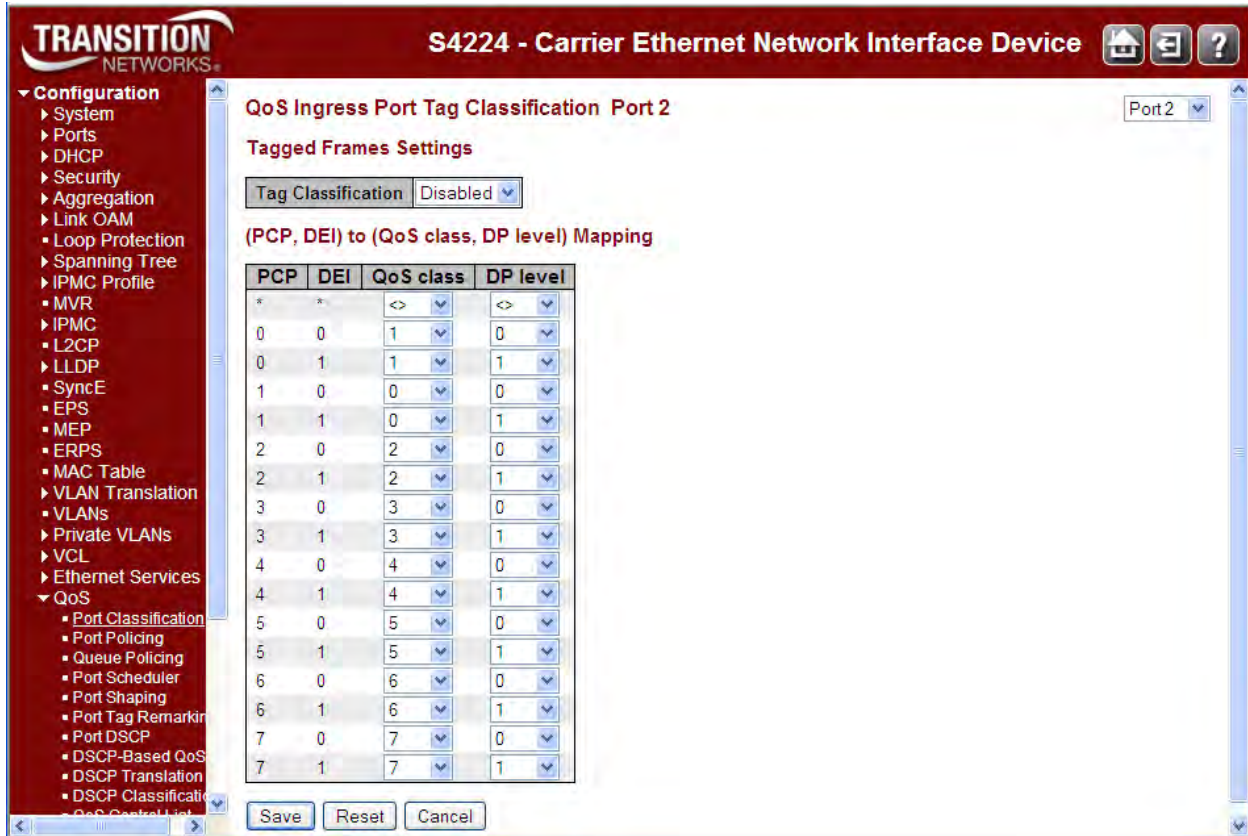
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Example

When you click the **Disabled** link in the **Tag Class.** column in a row for a port, the Tag Classification page displays for that port.



Here you can:

- Set **Tag Classification** to **Enabled** or **Disabled** (the default is **Disabled**),
- Set the (PCP, DEI) to (QoS class, DP level) Mapping:
 - Set **QoS class** to 0-7, and/or
 - Set **DP level** to 0 or 1.

You can click the browser's Back button to go back to the QoS Ingress Port Classification page.

Click the **Save** button when done; the QoS Ingress Port Classification page displays again with the new settings.

Port Policing

The **Configuration > QoS > Port Policing** menu path displays the QoS Ingress Port Policers table.

This page allows you to configure the Policer settings for all S4224 ports. The policer can limit the bandwidth of received frames. It is located in front of the Ingress queue. From the default page, check an **Enable** checkbox to begin configuration of Rate and Unit for Queue 0.

| Port | E | Queue 0 | Queue 1 | Queue 2 | Queue 3 | Queue 4 | Queue 5 | Queue 6 | Queue 7 |
|------|-------------------------------------|---------|---------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| | | Rate | Unit | Enable | Enable | Enable | Enable | Enable | Enable |
| * | <input type="checkbox"/> | 500 | <> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | <input checked="" type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 9 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 10 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 11 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

The displayed settings are explained below.

Port

The port number for which the configuration below applies. The * in the Port column acts as a 'wild card' character which causes the selections in this row to be applied to all other Ports (rows) in the table for which this selection is valid.

Enable (E)

Controls whether the policer is enabled on this S4224 port. Check the checkbox to enable port policing on this port (row). The default is unchecked (disabled).

Rate

Controls the rate for the policer. The default value is "500".

This value is restricted to 100-1000000 when the "Rate Unit" is "kbps" or "fps"

This value is restricted to 1-15000 when the Policer "Unit" is "Mbps" or "kfps".

Unit

Controls the unit of measure for the policer rate as kbps, Mbps, or fps. The default value is "kbps". (Where 'bps' is bits per second, and 'fps' is frames per second.)

Flow Control

Check or uncheck the checkbox to enable or disable Flow Control on a per-port basis. If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Queue Policing

The **Configuration > QoS > Queue Policing** menu path lets you configure the Queue Policer settings for all S4224 ports. Each policer can limit the bandwidth of received frames. A policer is located in front of the ingress queue. The default QoS Ingress Queue Policers page is shown below. From the default page, check an **Enable** checkbox to enable one or more Queue Policers starting at Queue 0.

| Port | E | Queue 0 | | Queue 1 | Queue 2 | Queue 3 | Queue 4 | Queue 5 | Queue 6 | Queue 7 |
|------|-------------------------------------|---------|------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| | | Rate | Unit | Enable | Enable | Enable | Enable | Enable | Enable | Enable |
| * | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | <input checked="" type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 9 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Note that the functions configured at Configuration > QoS are monitored at the Monitor > Ports menu path. For example:

Configure at

Configuration > QoS > QoS Control List
 Configuration > QoS > Port Policing
 Configuration > QoS > Queue Policing

Monitor at

Monitor > Ports > QCL Status
 Monitor > Ports > Detailed Statistics
 Monitor > Ports > QoS Statistics

The QoS Ingress Queue Policers parameters are explained below.

Port

The port number for which the configuration below applies. The first row in the table, marked by the * sign, enables or disables (checks or unchecks the 'enabled' checkbox) for all of the table rows.

Queue x Enable (E)

Check the checkbox to enable the queue policer on this S4224 port. This expands the table to let you define the rate(s) as shown below.

Rate

Controls the rate for the queue policer. The default value is 500. This value is restricted to 100 - 1000000 when the "Unit" is "kbps", and it is restricted to 1 - 3300 when the "Unit" is "Mbps". This field only displays if one or more of the queue policers are enabled.

Unit

Controls the unit of measure for the queue policer rate as kbps or Mbps. The default value is "kbps". This field only displays if one or more of the queue policers are enabled.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Example

The screen below shows multiple Queue Policers configured for port 2. The configuration below shows Port 2 with Queues 0, 1, and 2 enabled and Queue 0 is set for a rate of 10 Mbps and Queues 1 and 2 are set for 100Mbps.

| Port | Queue 0 | | | Queue 1 | | | Queue 2 | | | Queue 3 | Queue 4 | Queue 5 | Queue 6 | Queue 7 |
|------|-------------------------------------|------|------|-------------------------------------|------|------|-------------------------------------|------|------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| | E | Rate | Unit | E | Rate | Unit | E | Rate | Unit | Enable | Enable | Enable | Enable | Enable |
| * | <input type="checkbox"/> | 500 | <> | <input type="checkbox"/> | 500 | <> | <input type="checkbox"/> | 500 | <> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input checked="" type="checkbox"/> | 500 | kbps | <input checked="" type="checkbox"/> | 500 | kbps | <input checked="" type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Port Scheduler

The **Configuration > QoS > Port Scheduler** menu path displays the QoS Egress Port Schedulers table.

The screenshot shows the 'QoS Egress Port Schedulers' table with the following columns: Port, Mode, and Weight (subdivided into Q0, Q1, Q2, Q3, Q4, Q5). All 28 ports are currently set to 'Strict Priority' mode, and all weight values are '-'. A navigation menu on the left shows the path: Configuration > QoS > Port Scheduler.

| Port | Mode | Weight | | | | | |
|------|-----------------|--------|----|----|----|----|----|
| | | Q0 | Q1 | Q2 | Q3 | Q4 | Q5 |
| 1 | Strict Priority | - | - | - | - | - | - |
| 2 | Strict Priority | - | - | - | - | - | - |
| 3 | Strict Priority | - | - | - | - | - | - |
| 4 | Strict Priority | - | - | - | - | - | - |
| 5 | Strict Priority | - | - | - | - | - | - |
| 6 | Strict Priority | - | - | - | - | - | - |
| 7 | Strict Priority | - | - | - | - | - | - |
| 8 | Strict Priority | - | - | - | - | - | - |
| 9 | Strict Priority | - | - | - | - | - | - |
| 10 | Strict Priority | - | - | - | - | - | - |
| 11 | Strict Priority | - | - | - | - | - | - |
| 12 | Strict Priority | - | - | - | - | - | - |
| 13 | Strict Priority | - | - | - | - | - | - |
| 14 | Strict Priority | - | - | - | - | - | - |
| 15 | Strict Priority | - | - | - | - | - | - |
| 16 | Strict Priority | - | - | - | - | - | - |
| 17 | Strict Priority | - | - | - | - | - | - |
| 18 | Strict Priority | - | - | - | - | - | - |
| 19 | Strict Priority | - | - | - | - | - | - |
| 20 | Strict Priority | - | - | - | - | - | - |
| 21 | Strict Priority | - | - | - | - | - | - |
| 22 | Strict Priority | - | - | - | - | - | - |
| 23 | Strict Priority | - | - | - | - | - | - |
| 24 | Strict Priority | - | - | - | - | - | - |
| 25 | Strict Priority | - | - | - | - | - | - |
| 26 | Strict Priority | - | - | - | - | - | - |
| 27 | Strict Priority | - | - | - | - | - | - |
| 28 | Strict Priority | - | - | - | - | - | - |

Egress Scheduler and Shaper: Each port has an egress scheduler and a set of egress shapers. The scheduler on each port can operate in strict priority (the default) or in a mixed mode where the high priority queues are Strict and the rest are in DWRR (Deficit Weighted Round Robin).

The scheduler mode in DWRR lets you assign weights to the individual QoS queues. The Egress shapers available on a per-QoS queue basis provide shaping at a least granular level, and a port egress shaper provides an overall shaping and rate limiting the throughput.

Scheduler Mode (Strict Priority or Weighted)

Click on a linked port number (e.g., Port 1 above) to display the QoS Egress Port Scheduler and Shapers page.

At the Scheduler Mode dropdown, select **Weighted**.

The screenshot shows the configuration page for 'Port 28'. The 'Scheduler Mode' dropdown menu is open, showing three options: 'Strict Priority' (selected), 'Strict Priority', and '6 Queues Weighted'. Below the dropdown are 'Save', 'Reset', and 'Back' buttons.

6 Queues Weighted (Deficit Weighted Round Robin)

The DWRR uses a cost-based algorithm (compared to a weight-based algorithm). A high cost implies a small share of the bandwidth. When DWRR is enabled, each of the queues 5 through 0) are programmed with a cost (a number from 1 - 32). The programmable DWRR costs determine the behavior of the DWRR algorithm. The costs result in weights for each queue. The weights are relative to one another, and the resulting share of the egress bandwidth for a particular QoS class is equal to the queue's weight divided by the sum of all the queues' weights.

Costs can be converted to weights (and vice versa) with these two algorithms:

Weight to Cost: given a desired set of weights ($W_0, W_1, W_2, W_3, W_4, W_5$), calculate the costs using the following algorithm:

1. Set the cost of the queue with the smallest weight ($W_{smallest}$) to cost 32.
2. For any other queue Q_n with weight W_n , set the corresponding cost C_n to $C_n = 32 \times W_{smallest} / W_n$.

Cost to Weight: given a set of costs for all queues ($C_0, C_1, C_2, C_3, C_4, C_5$), then calculate the resulting weights using the following algorithm:

1. Set the weight of the queue with the highest cost ($C_{highest}$) to 1.
2. For any other queue Q_n with cost C_n , set the corresponding weight W_n to $W_n = C_{highest} / C_n$.

The **Configuration > QoS > Port Scheduler** menu path provides an overview of QoS Egress Port Schedulers for all S4224 ports.

The displayed QoS Egress Port Schedulers settings are described below.

Port

The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

Mode

Shows the scheduling mode for this port ("Strict Priority" or "Weighted"). Generally, Strict Priority (SP) queues are scheduled before WRR queues.

Strict Priority - The port transmits all packets out of higher priority queues before transmitting any from the lower priority queues.

Weighted - (WRR or Weighted Round Robin) - The port transmits a set number of packets from each queue, in a round robin fashion, so that each has a chance to transmit traffic.

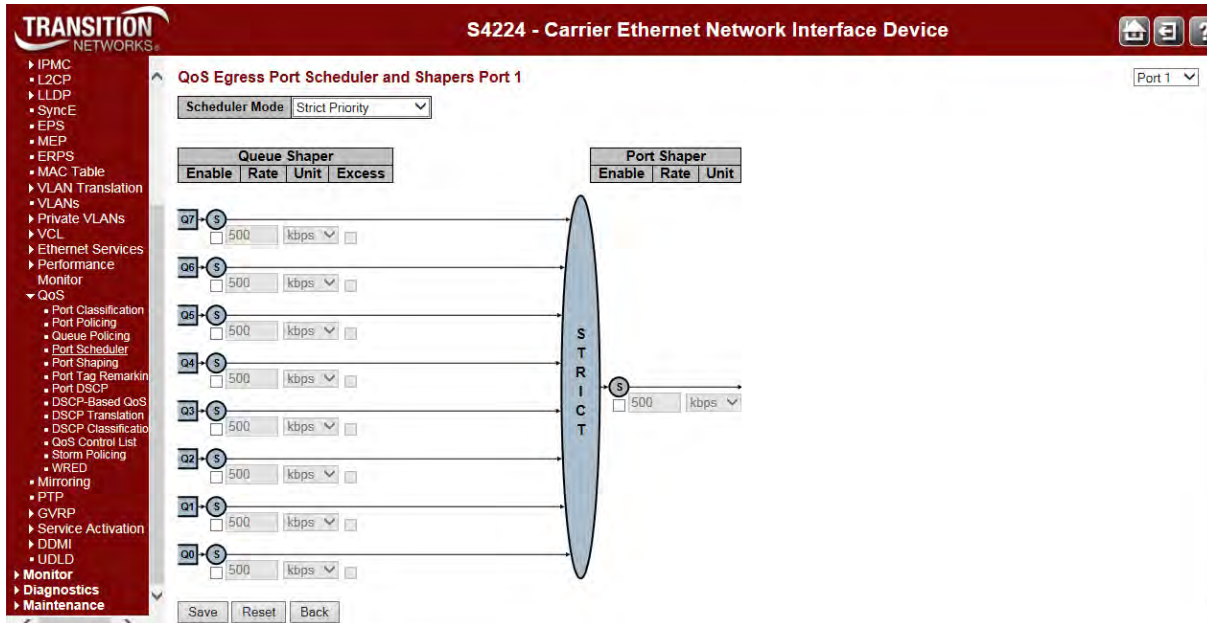
Weight (Q0 - Q5)

Shows the weight for this queue (Q0-Q5) and port (port 1-6).

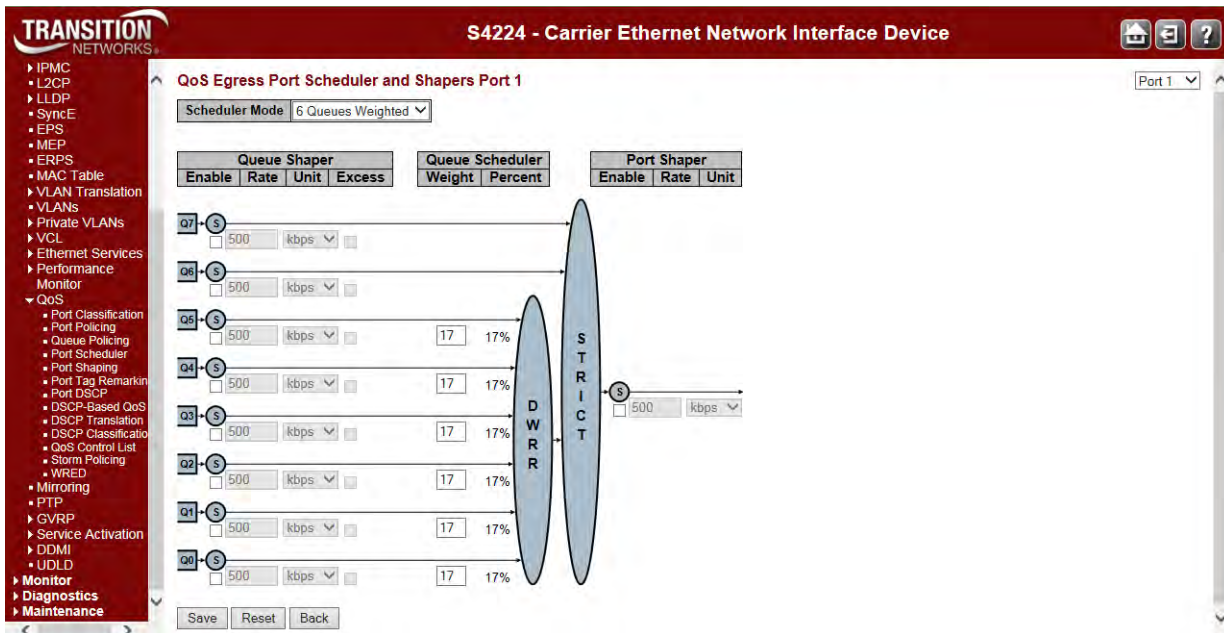
WRR setting examples for the number of packets transmitted from each queue are shown below. These values are permanent and you cannot change them.

| <u>Port Egress Queue</u> | <u>Max. No. of Packets</u> |
|--------------------------|----------------------------|
| Q3 | 8 |
| Q2 | 4 |
| Q1 | 2 |
| Q0 | 1 |

When you click on the Port number in a row, the QoS Egress Port Scheduler and Shapers for that Port display (e.g., for Port 1 in the screen sample below).



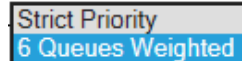
If Scheduler Mode is set to "6 Queues Weighted", then the Port Scheduler and Shapers for that Port display (e.g., for Port 1 as shown below).



The Port Scheduler and Shapers for a specific port are configured on this page. The parameters are explained below.

Scheduler Mode

Controls how many of the queues are scheduled as strict and how many are scheduled as weighted on this S4224 port. The dropdown options are **Strict Priority** or **6 Queues Weighted**.



Strict Priority
6 Queues Weighted

Queue Shaper Enable

Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate

Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".

Queue Shaper Unit

Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps". The default value is "kbps".

Queue Shaper Excess

Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight

Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent

Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Port Shaper Enable

Controls whether the port shaper is enabled for this switch port. Only shown for Non-service configuration.

Port Shaper Rate

Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps". Only shown for Non-service configuration.

Port Shaper Unit

Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps". Only shown for Non-service configuration.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Back: Click to undo any changes made locally and return to the previous page.

Port Shaping

The **Configuration > QoS > Port Shaping** menu path displays the QoS Egress Port Shapers page.

This page provides an overview of QoS Egress Port Shapers for all S4224 ports.

| Port | Shapers | | | | | | | Port | |
|--------------------|---------|----|----|----|----|----|----|------|----|
| | Q0 | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | | Q7 |
| 1 | - | - | - | - | - | - | - | - | - |
| 2 | - | - | - | - | - | - | - | - | - |
| 3 | - | - | - | - | - | - | - | - | - |
| 4 | - | - | - | - | - | - | - | - | - |
| 5 | - | - | - | - | - | - | - | - | - |
| 6 | - | - | - | - | - | - | - | - | - |
| 7 | - | - | - | - | - | - | - | - | - |
| 8 | - | - | - | - | - | - | - | - | - |
| 9 | - | - | - | - | - | - | - | - | - |
| 10 | - | - | - | - | - | - | - | - | - |
| 11 | - | - | - | - | - | - | - | - | - |
| 12 | - | - | - | - | - | - | - | - | - |
| 13 | - | - | - | - | - | - | - | - | - |
| 14 | - | - | - | - | - | - | - | - | - |
| 15 | - | - | - | - | - | - | - | - | - |
| 16 | - | - | - | - | - | - | - | - | - |
| 17 | - | - | - | - | - | - | - | - | - |

The displayed settings are explained below.

Port

The logical port number for the settings contained in the same row. Click on the port number to configure the port shapers for that port.

Shapers

Displays columns Q0 - Q7 and Port.

Qn

Shows "**disabled**" or the actual port shaper rate (e.g. "**800 Mbps**").

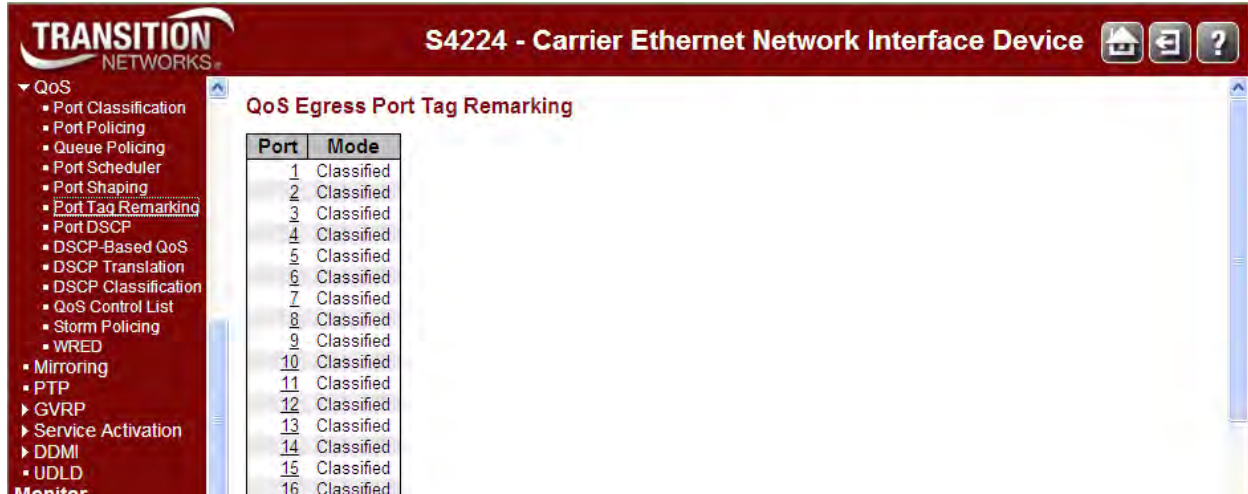
Port

Displays the current Port rate (e.g. "**500 kbps**") or "**disabled**".

Click on a port number link in the Port column (at the far left of the table) to display that port's "QoS Egress Port Scheduler and Shapers" (described earlier in this section). The Port column at the far right of the table displays the current port speed.

Port Tag Remarking

The **Configuration > QoS > Port Tag Remarking** menu path displays the QoS Egress Port Remarking page. This page provides an overview of QoS Egress Port Tag Remarking for all S4224 ports.



The displayed settings are explained below.

Port

The logical port for the settings contained in the same row. Click on the port number to configure tag remarking.

Mode

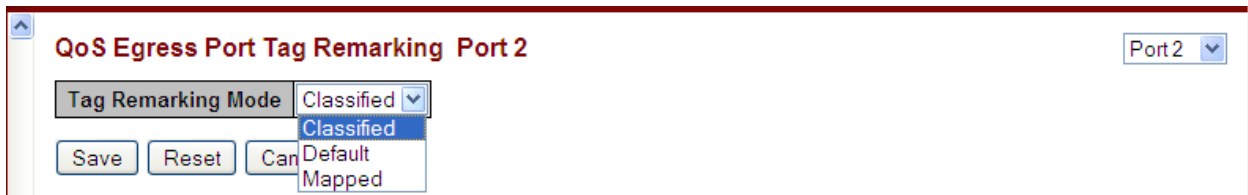
Shows the tag remarking mode for this port.

Classified: Use classified PCP/DEI values.

Default: Use default PCP/DEI values.

Mapped: Use mapped versions of QoS class and DP level.

When you click on the port number in a row, the **QoS Egress Port Tag Remarking** page for that port displays (**Port 2** in the example below).



The QoS Egress Port Tag Remarking for a specific port is configured on this page.

Tag Remarking Mode

Controls the tag remarking mode for this port.

Classified: Use classified PCP/DEI values.

Default: Use default PCP/DEI values. See example below.

Mapped: Use mapped versions of QoS class and DP level. See example below.

PCP/DEI Configuration

Controls the default PCP (0 - 7) and DEI (0, 1) values that display only when Tag Remarking Mode is set to **Default**, as shown below.

QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode: Default

PCP/DEI Configuration

| | |
|-------------|---|
| Default PCP | 0 |
| Default DEI | 0 |

Save Reset Cancel

Default PCP (Priority Code Point) is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority. The valid range is **0 - 7**. The default is **0**.

Default DEI (Drop Eligible Indicator) is a 1-bit field in the VLAN tag. The valid range is **0 - 1**. The default is **0**. Controls the default PCP and DEI values used when the **Tag Remarking Mode** (above) is set to **Default**.

When **0**, the DEI bit in the tag is set to **0** (the default setting).

When **1**, the DEI bit in the tag is set to the Classified DP level.

(QoS class, DP level) to (PCP, DEI) Mapping

Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to **Mapped** as shown below.

QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode: Mapped

(QoS class, DP level) to (PCP, DEI) Mapping

| QoS class | DP level | PCP | DEI |
|-----------|----------|-----|-----|
| * | * | <> | <> |
| 0 | 0 | 1 | 0 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 |
| 2 | 0 | 2 | 0 |
| 2 | 1 | 2 | 1 |
| 3 | 0 | 3 | 0 |
| 3 | 1 | 3 | 1 |
| 4 | 0 | 4 | 0 |
| 4 | 1 | 4 | 1 |
| 5 | 0 | 5 | 0 |
| 5 | 1 | 5 | 1 |
| 6 | 0 | 6 | 0 |
| 6 | 1 | 6 | 1 |
| 7 | 0 | 7 | 0 |
| 7 | 1 | 7 | 1 |

Save Reset Cancel

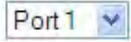
When **Tag Remarking Mode** is set to **Mapped**, the “(QoS class, DP level) to (PCP, DEI) Mapping” table displays. When **Tag Remarking Mode** is set to **Default**, the “PCP/DEI Configuration” table displays. You can click the browser’s back button to display the updated “QoS Egress Port Tag Remarking” page.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Click to undo any changes made locally and return to the previous page.

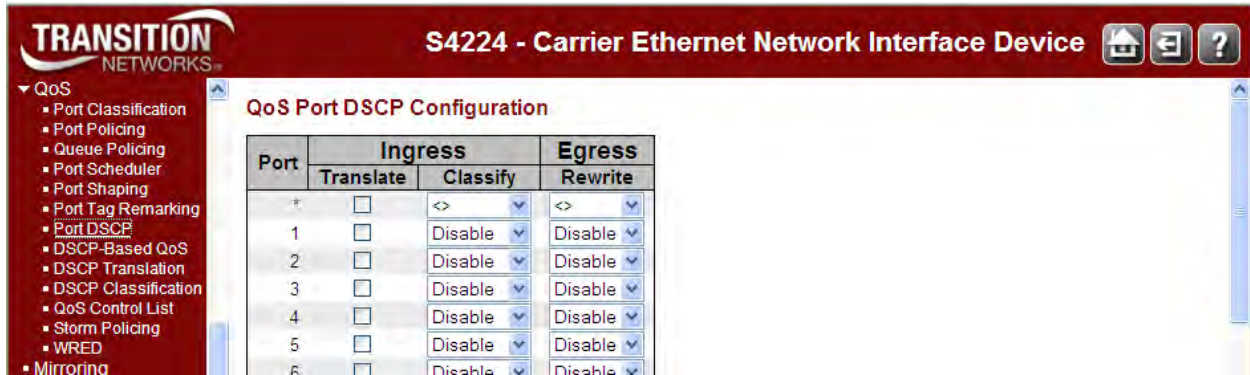
: Use the port select box to select which port details to display.

When the **Configuration > QoS > Port Tag Remarking** configuration is done, you can view the Queuing Counters at the **Monitor > Ports > QoS Statistics** menu path.

Port DSCP

You can configure S4224 QoS Port DSCP from the **Configuration > QoS > Port DSCP** menu path.

This page lets you configure the basic QoS Port DSCP Configuration settings for all S4224 ports. DSCP (Differentiated Services Code Point) is a field in the header of IP packets for packet classification purposes.



The Port DSCP parameters are explained below.

Port

The Port column shows the list of ports which you can configure DSCP ingress and egress settings.

Ingress

In Ingress settings you can change the ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress:

1. **Translate** : perform ingress translation for a specific port(s).
2. **Classify** perform ingress classification for a specific port(s).

Translate

To Enable the Ingress Translation click the checkbox.

Classify

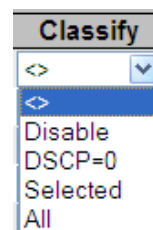
The Classification for a port can have one of these values:

Disable: No Ingress DSCP Classification.

DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.

Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.

All: Classify all DSCP.



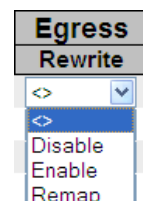
Egress / Rewrite

For Port Egress Rewriting select:

Disable: No Egress rewrite.

Enable: Rewrite enabled without remapping.

Remap: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.



Buttons

Save: Click to save changes.

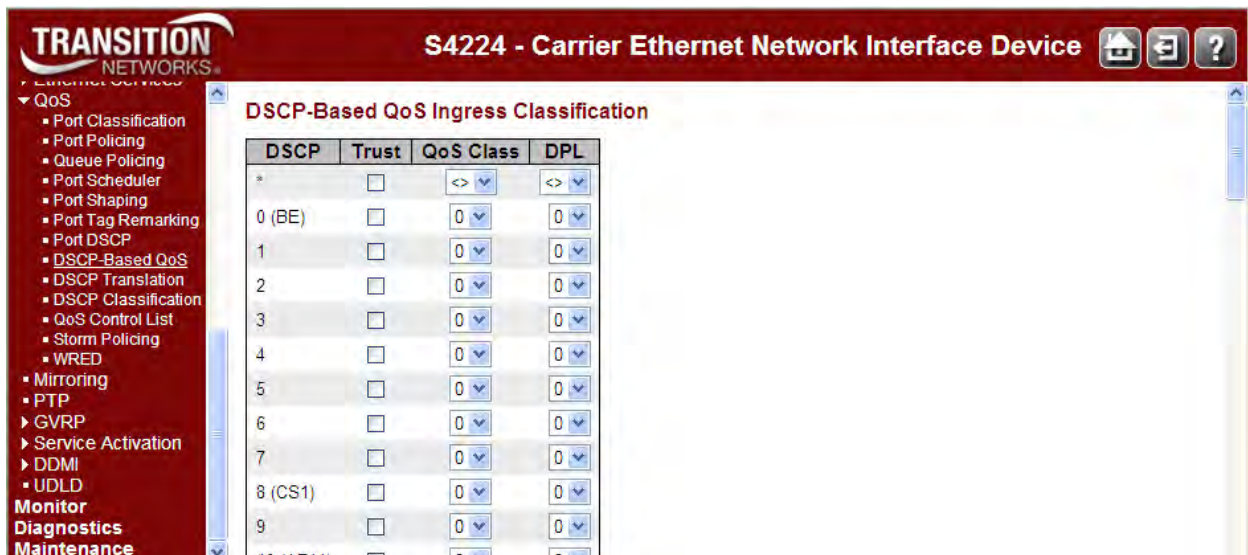
Reset: Click to undo any changes made locally and revert to previously saved values.

DSCP-Based QoS

The S4224 DSCP-based QoS Ingress Classification page is available from the **Configuration > QoS > DSCP-Based QoS** menu path. DSCP (Differentiated Services Code Point) is a field in the header of IP packets for packet classification purposes.

DSCP Traffic class (IP priority): If the ingress frame is an IP packet, then the priority is decided by the IP DSCP bits. This priority is used for all frames processing inside the device. Each of the 64 traffic classes can be marked as trusted or untrusted and the QoS Class and Drop priority level can be assigned.

This page lets you configure all of the S4224 QoS DSCP-based QoS Ingress Classification settings.



The displayed settings are explained below.

DSCP

The DiffServ standards define 64 DSCP values. Some of them are recommended for marking particular classes of QoS services (e.g. a value of 46 is usually recommended for real-time traffic with the strictest latency requirements).

Per the MEF, DiffServ defines several per-hop behaviors (PHBs) that provide robust QoS capabilities compared to other methods. DiffServ provides 64 different values called DiffServ Code Points, or DSCPs, that are used to determine the Class of Service (CoS). EF (Expedited Forwarding) for low delay / low loss service, AF (Assured Forwarding) in four classes for bursty real time and non-real time services, CS (Class Selector) for partial backward compatibility with IP TOS, and DF (Default Forwarding) for best effort services.

The maximum number of supported DSCP values is 64. In the DSCP column, the DSCP Name can be **BE**, **CSx**, **EFx**, or **AFx** where:

AF refers to Assured Forwarding is provided in four classes for bursty real time and non-real time services.

BE: refers to Standard (Best Effort) forwarding.

CS refers to the Class Selector (per [RFC 2474](#)).

EF refers to the Expedited Forwarding ([RFC 3246](#)). The EF PHB has the characteristics of low delay, low loss and low jitter. These characteristics are suitable for voice, video and other real-time services.

Three fundamental forwarding behaviors are defined for general use by IETF [RFC 4594](http://tools.ietf.org/html/rfc4594): basic Default Forwarding (DF) behavior for elastic traffic, Assured Forwarding (AF) behavior, and Expedited Forwarding (EF) behavior for real-time (inelastic) traffic. For additional information see the RFC at <http://tools.ietf.org/html/rfc4594>.

Trust

Check the **Trust** checkbox if the DSCP value is trusted. This controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.

To use DSCP requires some sort of trust between routers. Generally, DSCP values are assigned by the edge routers of an administrative domain (e.g. a Regional Network) and used by the core routers of the same domain. If there is no trust relationship between domains, the edge routers of each domain may re-assign DSCP values of ingress packets if they are already marked with a non-default (non-zero) value. This would prevent, for example, one domain transmitting all the packets with a DSCP value indicating priority treatment into another domain and overloading that network's priority service. A worse example could be where the DSCP value for low priority in one domain is used to mean higher priority in another. Without inspecting and re-marking the inbound DSCP values, both networks would give the opposite treatment to packets than was intended.

Some applications (e.g., VoIP or videoconferencing) mark packets by non-default DSCP values when they are generated by the application's host computer. This might be an IP phone or a videoconferencing client – although the default DSCP marking may not be consistent with the network scheme. So while this may at first seem to remove the need for an intermediate node (for example, a router) to classify the packet, the intermediate node may actually need to inspect the packets and re-mark the DSCP field.

QoS Class

Enter the QoS Class value (0-7) at the dropdown. Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one-to-one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

DPL

Enter the Drop Precedence Level (0-1) at the dropdown. Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level.

A DP level of 0 (zero) corresponds to 'Committed' (Green) frames (the default).

A DP level of 1 or higher corresponds to 'Discard Eligible' (Yellow) frames.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

DSCP Translation

The DSCP Translation page is available from the **Configuration > CoS > DSCP Translation** menu path. DSCP (Differentiated Services Code Point) is a field in the header of IP packets for packet classification purposes.

The S4224 can operate as a DS boundary which can translate different domains' DSCP values. It provides classification to a remapped DSCP value or translates to a new DSCP value on ingress and also at egress it can remap to a DSCP value along with the ability to set the drop precedence level. To perform the DSCP translation, the port associated with ingress/egress also needs to enable remarking accordingly.

This page lets you configure basic QoS DSCP Translation settings. DSCP translation can be performed on Ingress or Egress.

| DSCP | Ingress | | Egress |
|-----------|-----------|--------------------------|-----------|
| | Translate | Classify | Remap |
| * | <> | <input type="checkbox"/> | <> |
| 0 (BE) | 0 (BE) | <input type="checkbox"/> | 0 (BE) |
| 1 | 1 | <input type="checkbox"/> | 1 |
| 2 | 2 | <input type="checkbox"/> | 2 |
| 3 | 3 | <input type="checkbox"/> | 3 |
| 4 | 4 | <input type="checkbox"/> | 4 |
| 5 | 5 | <input type="checkbox"/> | 5 |
| 6 | 6 | <input type="checkbox"/> | 6 |
| 7 | 7 | <input type="checkbox"/> | 7 |
| 8 (CS1) | 8 (CS1) | <input type="checkbox"/> | 8 (CS1) |
| 9 | 9 | <input type="checkbox"/> | 9 |
| 10 (AF11) | 10 (AF11) | <input type="checkbox"/> | 10 (AF11) |
| 11 | 11 | <input type="checkbox"/> | 11 |

The displayed settings are explained below.

DSCP

A maximum of 64 DSCP values are supported and the valid DSCP values are 0 to 63.

The DSCP value can include **BE**, **CSx**, **EFx**, or **AFx** where:

AF refers to Assured Forwarding is provided in four classes for bursty real time and non-real time services.

BE: refers to Standard (Best Effort) forwarding.

CS refers to the Class Selector (per [RFC 2474](#)).

EF refers to the Expedited Forwarding ([RFC 3246](#)). The EF PHB has the characteristics of low delay, low loss and low jitter. These characteristics are suitable for voice, video and other real-time services.

Three fundamental forwarding behaviors are defined for general use by IETF [RFC 4594](#): basic Default Forwarding (DF) behavior for elastic traffic, Assured Forwarding (AF) behavior, and Expedited Forwarding (EF) behavior for real-time (inelastic) traffic. For additional information see the RFC at <http://tools.ietf.org/html/rfc4594>.

Ingress

Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation on the Ingress side:

Translate: DSCP at the Ingress side can be translated to DSCP values of 0-63.

Classify: Check to enable Classification at the Ingress side.

Egress

The following configurable parameter is for the Egress side:

Remap: Select the DSCP value from select menu to which you want to remap. Valid DSCP values are 0 - 63.

The Egress Remap here refers to the remapping of the Drop precedence at 0 level or 1 level (when the classified DSCP marked traffic Ingresses). The Drop precedence determines the packet discard behavior in the case of congestion within a classified traffic.

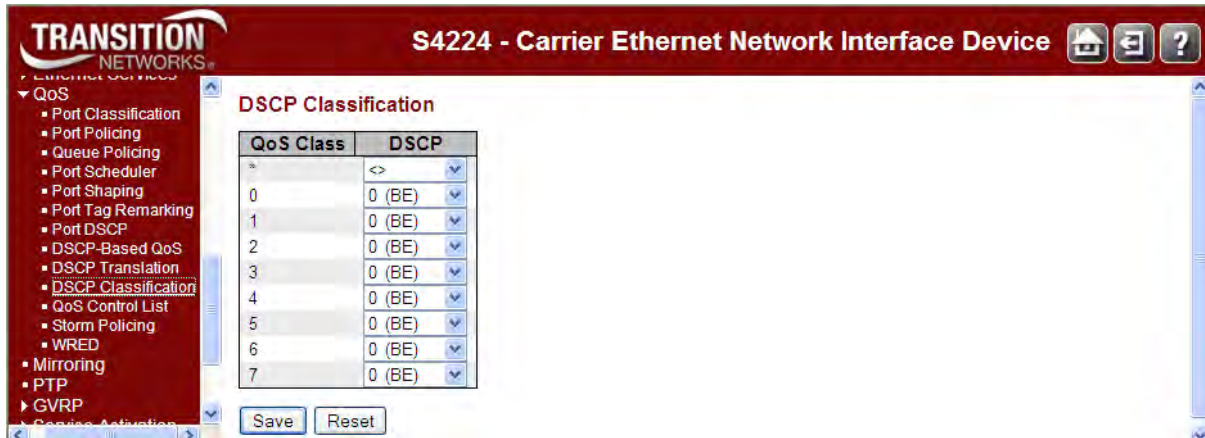
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

DSCP Classification

The DSCP Classification page is available from the **Configuration > QoS > DSCP Classification** menu path. The DSCP Classification page lets you configure the mapping of QoS class and Drop Precedence Level to DSCP value.



The displayed settings are explained below.

QoS Class

Actual QoS class (0 - 7).

DSCP

Select the classified DSCP value (0 - 63).

DPL: For Drop Precedence Level DP0 and DP1. Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. A DP level of 0 (zero) corresponds to 'Committed' (Green) frames. A DP level of 1 or higher corresponds to 'Discard Eligible' (Yellow) frames.

DSCP: The DiffServ standards define 64 DSCP values. Some of them are recommended for marking particular classes of QoS services (e.g., a value of 46 is usually recommended for real-time traffic with the strictest latency requirements). The maximum number of supported DSCP values is 64.

In the DSCP column, the DSCP value can be **BE**, **CSx**, **EFx**, or **AFx** where:

AF refers to Assured Forwarding.

BE: refers to Standard (Best Effort) forwarding.

CS refers to the Class Selector (per [RFC 2474](http://tools.ietf.org/html/rfc2474)).

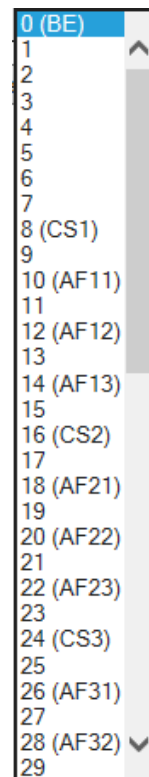
EF refers to the Expedited Forwarding ([RFC 3246](http://tools.ietf.org/html/rfc3246)).

Three fundamental forwarding behaviors are defined for general use by IETF [RFC 4594](http://tools.ietf.org/html/rfc4594): basic Default Forwarding (DF) behavior for elastic traffic, Assured Forwarding (AF) behavior, and Expedited Forwarding (EF) behavior for real-time (inelastic) traffic. For additional information see the RFC at <http://tools.ietf.org/html/rfc4594>.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.



QoS Control List (QCL)

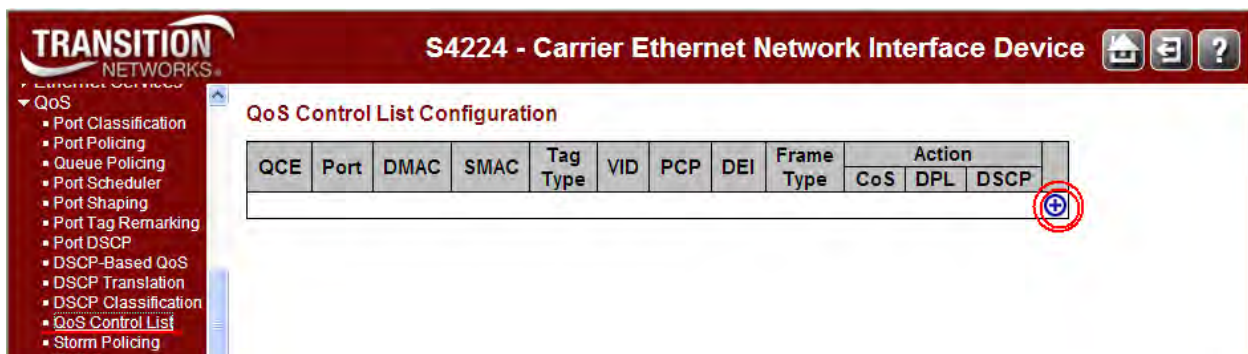
The QoS Control List page is available from the **Configuration > QoS > QoS Control List** menu path. A QCL (QoS Control List) is the list table of QCEs containing QoS control entries that classify to a specific QoS class on specific traffic objects. Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class. A QCE (QoS Control Entry) describes the QoS class associated with a particular QCE ID.

Advanced per flow QoS: Apart from the basic QoS classification mentioned above, a QCL is provided to choose any traffic flow based on Layer 2 -4 packet headers and classify then to a particular QoS class. A complete configuration option for type of flow and the various QoS values are provided as a QCE. Some of the often used flows are VLAN based service, IP flows, TCP sessions, etc.

The QCL Configuration is a table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects. QoS class associated with a particular QCE ID. There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

The QoS Control List configuration page shows the QoS Control List (QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The S4224 supports up to 1024 QCEs.

From the default QoS Control List Configuration page, click on the plus sign (+) to add a new QCE to the list.



The displayed settings are explained below.

QCE

Indicates the QCE ID.

Port

Indicates the list of ports configured with the QCE.

DMAC

Indicates the destination MAC address. Possible values are:

Any: Match any DMAC.

Unicast: Match unicast DMAC.

Multicast: Match multicast DMAC.

Broadcast: Match broadcast DMAC.

Specific: Match specific DMAC.

The default value is 'Any'.

| |
|-----------|
| Any |
| Unicast |
| Multicast |
| Broadcast |
| Specific |

SMAC

Match a **Specific** source MAC address or '**Any**'. If a port is configured to match on DMAC/DIP, this field indicates the DMAC.

Tag Type

Indicates/sets the tag type. Possible values are:

Any: Match tagged and untagged frames.

Untagged: Match untagged frames.

Tagged: Match tagged frames.

C-Tagged: Match C-tagged frames.

S-Tagged: Match S-tagged frames.

The default value is '**Any**'.

| |
|----------|
| Any |
| Untagged |
| Tagged |
| C-Tagged |
| S-Tagged |

VID

Indicates (VLAN ID), either a **Specific** VID or **Range** of VIDs. VID can be in the range 1-4095 or '**Any**'.

PCP

Priority Code Point: Valid values of PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or '**Any**'.

DEI

Drop Eligible Indicator: Valid value of DEI are 0, 1 or '**Any**'.

Inner Tag

Indicates/sets the inner tag type. Possible values are:

Any: Match tagged and untagged frames.

Untagged: Match untagged frames.

Tagged: Match tagged frames.

C-Tagged: Match C-tagged frames.

S-Tagged: Match S-tagged frames.

The default value is '**Any**'.

| |
|----------|
| Any |
| Untagged |
| Tagged |
| C-Tagged |
| S-Tagged |

Inner VID

Select '**Any**', '**Specific**', or '**Range**' as the Inner VLAN ID type. The default is '**Any**'. Selecting 'Specific' or 'Range' will present additional entry options.

| |
|----------|
| Any |
| Specific |
| Range |

Inner PCP

Select Any, 0, 1, 2, 3, 4, 5, 6, 7, 0-1, 2-3, 4-5, 6-7, 0-3, or 4-7 as the inner PCP value.

Inner DEI

Select Any, 0, or 1 as the inner DEI value.

Frame Type

Indicates the type of frame to look for incoming frames. Valid frame types are:

Any: The QCE will match all frame types.

Ethertype: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.

LLC: Only (LLC) frames are allowed.

SNAP: Only (SNAP) frames are allowed.

IPv4: The QCE will match only IPV4 frames.

IPv6: The QCE will match only IPV6 frames.

| |
|-----------|
| Any |
| EtherType |
| LLC |
| SNAP |
| IPv4 |
| IPv6 |

Action Parameters

Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:

CoS: Class of Service (**0-7**) or **'Default'**.

DPL: Drop Precedence Level (**0-3**) or **'Default'**.

DSCP: (**0-63**, **BE**, **CS1-CS7**, **EF** or **AF11-AF43**) or **'Default'**.


'Default' means that the default classified value is not modified by this QCE.


Action Parameters


| | |
|------|-----------|
| CoS | Default ▾ |
| DPL | Default ▾ |
| DSCP | Default ▾ |


Modification Buttons

You can modify each QCE (QoS Control Entry) in the table using the following buttons:


: Inserts a new QCE before the current row.

: Edits the QCE.

: Moves the QCE up the list.


: Moves the QCE down the list.

: Deletes the QCE.

: The lowest plus sign adds a new entry at the bottom of the QCE listings.

Buttons

Refresh: Click to refresh the page. This will help to check the latest conflict status after releasing the resources.

When you click on the lowest plus sign () to add a new QCE to the end of the list, a parameters screen displays.

Examples

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

QCE Configuration

| Port Members | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Key Parameters

| | |
|------------|-----|
| DMAC | Any |
| SMAC | Any |
| Tag | Any |
| VID | Any |
| PCP | Any |
| DEI | Any |
| Frame Type | Any |

Action Parameters

| | |
|------|---------|
| CoS | 0 |
| DPL | Default |
| DSCP | Default |

Save Reset Cancel

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

QCE Configuration

| Port Members | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Key Parameters

| | | |
|------------|-----------|----------|
| DMAC | Unicast | |
| SMAC | Specific | 00-22-00 |
| Tag | Untagged | |
| VID | Any | |
| PCP | Any | |
| DEI | Any | |
| Frame Type | EtherType | |

Action Parameters

| | |
|------|---------|
| CoS | 1 |
| DPL | 1 |
| DSCP | 8 (CS1) |

EtherType Parameters

| | | |
|------------|----------|---------------|
| Ether Type | Specific | Value: 0xFFFF |
|------------|----------|---------------|

Save Reset Cancel

You can click the browser's Back button to return to the QoS Control List page, or edit the parameters and click **Save**.

Sample Parameters

QCE Configuration

| Port Members | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Key Parameters

| | |
|------------|-----|
| DMAC | Any |
| SMAC | Any |
| Tag | Any |
| VID | Any |
| PCP | Any |
| DEI | Any |
| Frame Type | Any |

Action Parameters

| | |
|------|---------|
| CoS | Default |
| DPL | Default |
| DSCP | Default |

Note that not all of the parameters will display in all situations. The **Frame Type** selection (in the **Key Parameters** table) determines which specific subset of parameters display.

Frame Types

| Key Parameter | Additional Parameters | Additional Parameter Values | | | | | | |
|------------------------|--|-----------------------------|-----|--------------|-----|---------|-----|---|
| Frame Type = Any | No additional parameters displayed. | N/A | | | | | | |
| Frame Type = EtherType | <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;"> Frame Type EtherType </div> <p style="color: red; margin: 0;">EtherType Parameters</p> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;"> Ether Type Any </div> | EtherType = Any or Specific | | | | | | |
| Frame Type = LLC | <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;"> Frame Type LLC </div> <p style="color: red; margin: 0;">LLC Parameters</p> <table border="1" style="width: 100%; border-collapse: collapse; margin-bottom: 5px;"> <tr><td>DSAP Address</td><td>Any</td></tr> <tr><td>SSAP Address</td><td>Any</td></tr> <tr><td>Control</td><td>Any</td></tr> </table> | DSAP Address | Any | SSAP Address | Any | Control | Any | SSAP Address = Any or Specific DSAP Address = Any or Specific Control = Any or Specific |
| DSAP Address | Any | | | | | | | |
| SSAP Address | Any | | | | | | | |
| Control | Any | | | | | | | |
| Frame Type = SNAP | <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;"> Frame Type SNAP </div> <p style="color: red; margin: 0;">SNAP Parameters</p> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;"> PID Any </div> | PID = Any or Specific | | | | | | |

| | | | | | | | | | | |
|---------------------------------|--|----------|-----|--------------|-----|-------------|-----|---|-----|---|
| <p>Frame Type = IPv4</p> | <p>Frame Type IPv4 </p> <p>IPv4 Parameters</p> <table border="1"> <tr><td>Protocol</td><td>Any</td></tr> <tr><td>SIP</td><td>Any</td></tr> <tr><td>IP Fragment</td><td>Any</td></tr> <tr><td>DSCP</td><td>Any</td></tr> </table> | Protocol | Any | SIP | Any | IP Fragment | Any | DSCP | Any | <p>Protocol = Any, UDP, TCP, Other</p> <p>SIP = Any or Specific</p> <p>IP Fragment = Any, Yes, or No</p> <p>DSCP = Any, Specific or Range</p> |
| Protocol | Any | | | | | | | | | |
| SIP | Any | | | | | | | | | |
| IP Fragment | Any | | | | | | | | | |
| DSCP | Any | | | | | | | | | |
| <p>Frame Type = IPv6</p> | <p>Frame Type IPv6 </p> <p>IPv6 Parameters</p> <table border="1"> <tr><td>Protocol</td><td>Any</td></tr> <tr><td>SIP (32 LSB)</td><td>Any</td></tr> <tr><td>DSCP</td><td>Any</td></tr> </table> | Protocol | Any | SIP (32 LSB) | Any | DSCP | Any | <p>Protocol = Any, UDP, TCP, or Other</p> <p>SIP (32 LSB) = Any or Specific</p> <p>DSCP = Any, Specific or Range</p> | | |
| Protocol | Any | | | | | | | | | |
| SIP (32 LSB) | Any | | | | | | | | | |
| DSCP | Any | | | | | | | | | |

The QoS Control List configuration page lets you insert and edit a single QoS Control Entry at a time. A QCE consists of several parameters. These parameters vary according to the frame type that you select.

Select the switch member the QCE will be added. It can be any specific switch by switch ID or 'Any' in which case QCE will be applied to all the switches in the stack.

Port Members

Check the checkbox button to include the port in the QCL entry. By default all ports are included.

Key Parameters

Key configuration is described below:

DMAC Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast', 'Specific' (xx-xx-xx-xx-xx-xx) or 'Any'.

SMAC Source MAC address: xx-xx-xx-xx-xx-xx or 'Any'.

Tag Value of Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.

VID Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.

PCP Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI Valid value of DEI can be '0', '1' or 'Any'.

Frame Type Frame Type can have any of the following values:

1. Any
2. EtherType
3. LLC
4. SNAP
5. IPv4
6. IPv6

Note: These frame types are explained below.

1. Any

Allow all types of frames.

2. EtherType

Ether Type Valid EtherTypes are 0x600-0xFFFF excluding 0x800 (IPv4) and 0x86DD (IPv6) or 'Any'.

3. LLC

SSAP Address Valid SSAP (Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.

DSAP Address Valid DSAP (Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'.

Control Valid Control field can vary from 0x00 to 0xFF or 'Any'.

4. SNAP

PID Valid PID (a.k.a Ether Type) can be 0x0000-0xFFFF or 'Any'.

5. IPv4

Protocol IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.

Source IP Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero.

IP Fragment IPv4 frame fragmented option: 'Yes', 'No' or 'Any'.

DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

Sport Source TCP/UDP port: (0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

6. IPv6

Protocol IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.

Source IP 32 LS bits of IPv6 source address in value/mask format or 'Any'.

DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

Sport Source TCP/UDP port: (0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Action Parameters

CoS Class of Service: (0-7) or 'Default'.

DP Drop Precedence Level: (0-1) or 'Default'.

DSCP DSCP: (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.

'Default' means that the default classified value is not modified by this QCE.

Buttons

Save: Click to save the configuration and move to main QCL page.

Reset: Click to undo any changes made locally and revert to previously saved values.

Cancel: Return to the previous page without saving the configuration change.

Storm Policing

The S4224 Port Storm **Policer** is configured from the **Configuration > QoS > Storm Policing** menu path at the **Port Storm Policer Configuration** page.

There is a storm policer for unicast frames, broadcast frames and unknown (flooded) frames.

| Port | Unicast Frames | | | Broadcast Frames | | | Unknown Frames | | |
|------|--------------------------|------|------|--------------------------|------|------|--------------------------|------|------|
| | Enable | Rate | Unit | Enable | Rate | Unit | Enable | Rate | Unit |
| * | <input type="checkbox"/> | 500 | <> | <input type="checkbox"/> | 500 | <> | <input type="checkbox"/> | 500 | <> |
| 1 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 2 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 3 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 4 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 5 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 6 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 7 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 8 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 9 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 10 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 11 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 12 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |
| 13 | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps | <input type="checkbox"/> | 500 | kbps |

A traffic storm occurs when packets flood a LAN, creating excessive traffic which degrades network performance. The Storm Control feature prevents ports from being disrupted by a broadcast, multicast, or unicast traffic storm on a physical interface. Storm Control monitors incoming traffic levels over a selected traffic storm control rate and, during the interval, compares the traffic level with the selected traffic storm control level. Each port has traffic storm control levels that are used for each traffic type (Unicast, Multicast, and Broadcast). When the ingress traffic for which Storm Control is enabled reaches the traffic storm control rate you configured on the port, Storm Control drops traffic until the Storm Control interval ends. A higher rate allows more packets to pass through without dropping traffic.

Note: Frames sent to the S4224 CPU are limited to approximately 4 kpps (e.g., Management VLAN broadcasts are limited to this rate). The Management VLAN is configured at **Configuration > System > IP**.

Port

The port number for which the configuration below applies.

Enable

Enable or disable the storm policer for this switch port.

Rate

Controls the rate for the **port** storm policer. This value is restricted to 1-13128072 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the port storm policer.

Unit

Controls the unit of measure for the port storm policer rate as fps, kfps, kbps or Mbps.

Storm control only works on Inbound packets; it does not prevent a port from being overwhelmed with broadcasts from the core or from other access switches.

Note: Follow your organization's policies and procedures and best practices for implementing storm control (e.g., if you should set the Multicast limit higher than the Broadcast limit, or at least set them equal, etc.).

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

WRED (Weighted Random Early Detection) Configuration

The **Configuration > QoS > WRED** menu path lets you configure the Random Early Detection (RED) settings for queues 0 to 5.

RED cannot be applied to queue 6 and 7. Through different RED configuration for the queues (QoS classes) it is possible to obtain Weighted Random Early Detection (WRED) operation between queues. The settings are global for all ports in the device.

| Queue | Enable | Min | Max DP 1 | Max DP 2 | Max DP 3 |
|-------|--------------------------|-----|----------|----------|----------|
| 0 | <input type="checkbox"/> | 0 | 1 | 5 | 10 |
| 1 | <input type="checkbox"/> | 0 | 1 | 5 | 10 |
| 2 | <input type="checkbox"/> | 0 | 1 | 5 | 10 |
| 3 | <input type="checkbox"/> | 0 | 1 | 5 | 10 |
| 4 | <input type="checkbox"/> | 0 | 1 | 5 | 10 |
| 5 | <input type="checkbox"/> | 0 | 1 | 5 | 10 |

The displayed settings are:

Queue

The queue number (QoS class) for which the configuration below applies.

Enable

Controls whether RED is enabled for this queue.

Min

Controls the lower RED threshold. If the average queue filling level is below this threshold, the drop probability is zero. This value is restricted to **0-100**. The default is **0**.

Max DP 1

Controls the drop probability for frames marked with Drop Precedence Level 1 when the average queue filling level is 100%. This value is restricted to **0-100**. The default is **1**.

Max DP 2

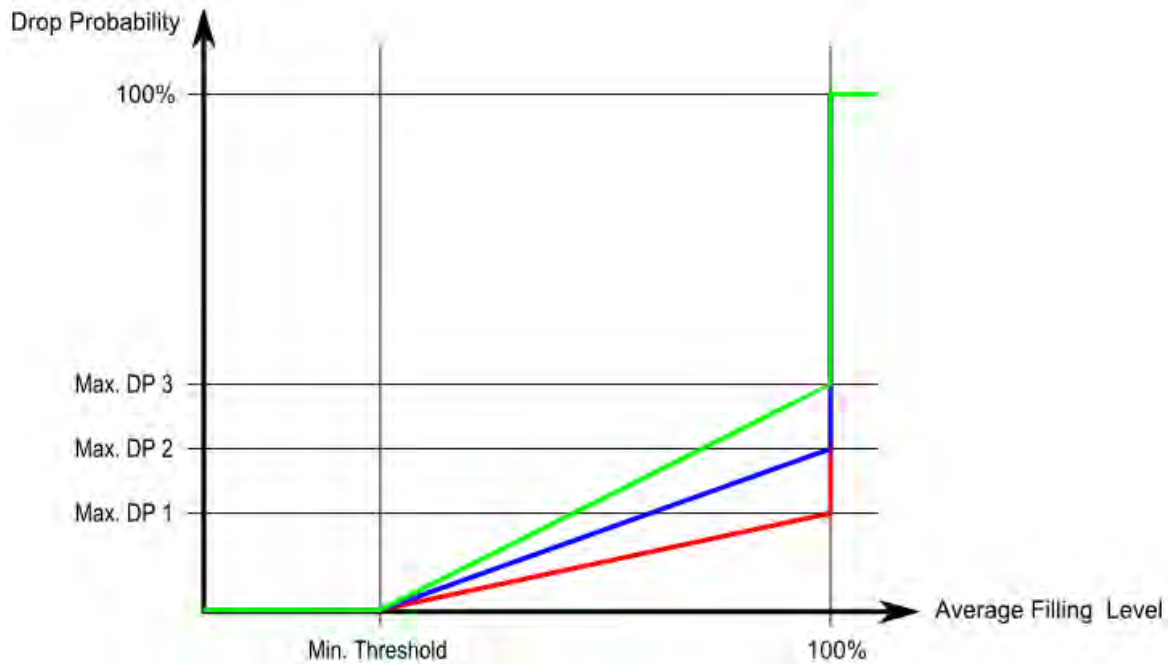
Controls the drop probability for frames marked with Drop Precedence Level 2 when the average queue filling level is 100%. This value is restricted to **0-100**. The default is **5**.

Max DP 3

Controls the drop probability for frames marked with Drop Precedence Level 3 when the average queue filling level is 100%. This value is restricted to **0-100**. The default is **10**.

RED Drop Probability Function

The following illustration shows the drop probability function with associated parameters.



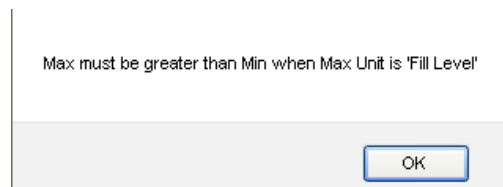
Max DP 1-3 is the drop probability when the average queue filling level is 100%. Frames marked with Drop Precedence Level 0 are never dropped. Min is the average queue filling level where the queues randomly start dropping frames. The drop probability for frames marked with Drop Precedence Level n increases linearly from zero (at Min average queue filling level) to Max DP n (at 100% average queue filling level).

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Messages: *Max. must be greater than Min when Max Unit is 'Fill Level'.*



Mirroring & Remote Mirroring Configuration

For debugging network problems or monitoring network traffic, the S4224 system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

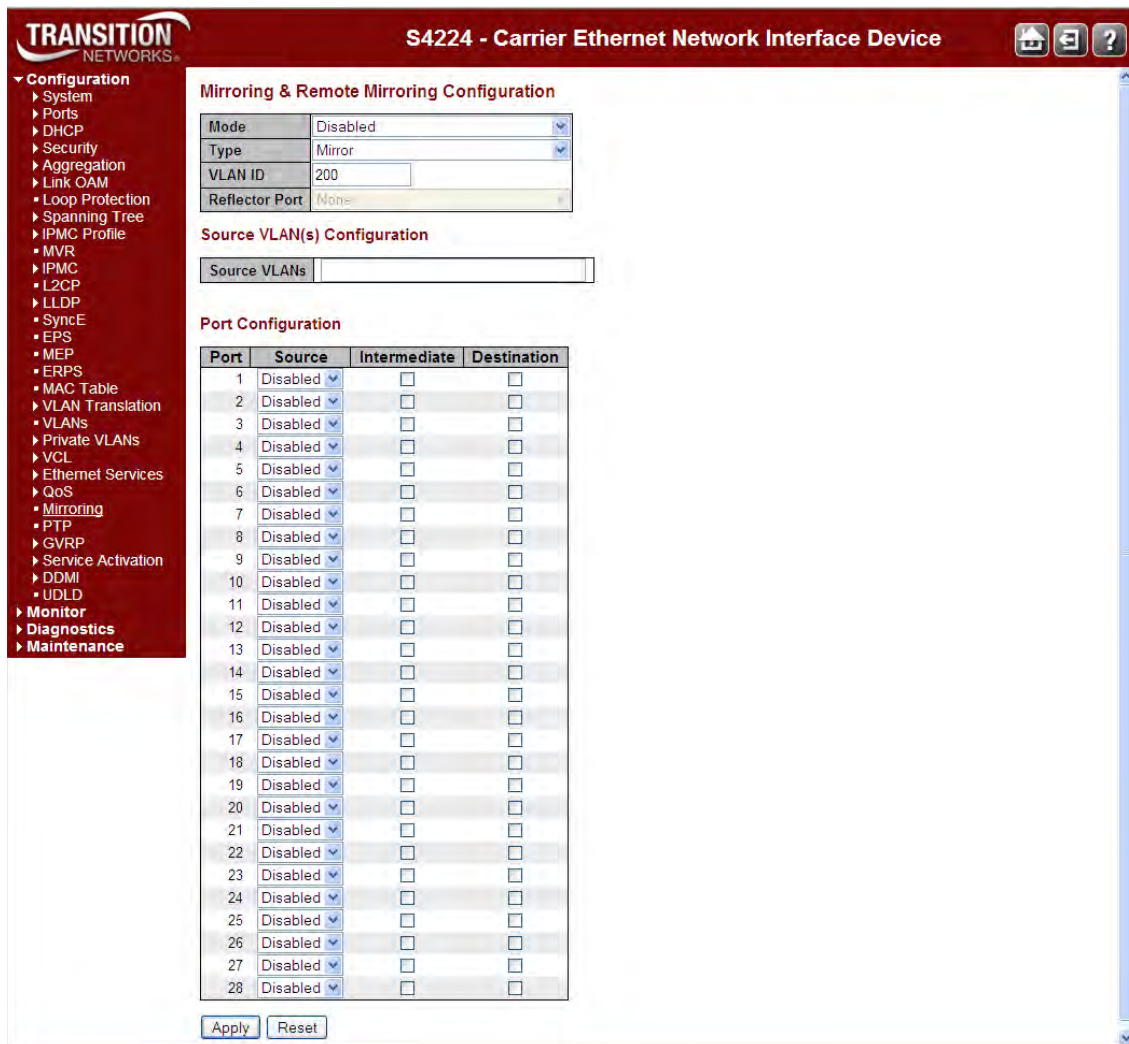
Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

Mirroring is a feature for switched port analyzer. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

Remote Mirroring is an extended function of Mirroring. It can extend the destination port so an administrator can analyze the network traffic on other switches.

If you want to get the tagged mirrored traffic, you set VLAN egress tagging as "Tag All" on the reflector port. On the other hand, if you want to get untagged mirrored traffic, you set VLAN egress tagging as "Untag ALL" on the reflector port.

Navigate to the **Configuration > Mirroring** menu path to display the default Mirroring & Remote Mirroring Configuration page.



Mirroring & Remote Mirroring Configuration

Mode

Select to Enable or Disable the Mirror or Remote Mirroring function.

Type

Select the switch type:

Mirror: The switch is running in mirror mode. The source port(s) and destination port are located on this switch.

Source: The switch is a source node for monitor flow. The source port(s), reflector port and intermediate port(s) are located on this switch.

Intermediate: The switch is a forwarding node for monitor flow and the switch is an option node. The object is to forward traffic from source switch to destination switch. The intermediate ports are located on this switch.

Destination: The switch is an end node for monitor flow. The destination port(s) and intermediate port(s) are located on this switch.

| |
|-----------------------|
| Mirror |
| Source(RMirror) |
| Intermediate(RMirror) |
| Destination(RMirror) |

VLAN ID

The VLAN ID points to where the monitor packet will copy to.

Reflector Port

The reflector port is a method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until Remote Mirroring is disabled. If you shut down a port, it cannot be a candidate for reflector port. If you shut down the port which is a reflector port, the Remote Mirror function cannot work.

Note 1: The reflector port requires you to select "Source" as the switch "Type" (see above).

Note 2: The reflector port requires you to disable MAC Table learning and STP.

Note 3: The reflector port only supports pure copper ports.

| |
|--------|
| Port 1 |
| Port 2 |
| Port 3 |
| Port 4 |

Source VLAN(s) Configuration

The switch can support VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs in this field. **Note:** the Mirroring session must have either ports or VLANs as sources, but not both.

Port Configuration (Remote Mirroring)

The following table is used for port role selecting.

Port

The logical port for the settings contained in the same row.

Source

Select the Mirror mode:

Disabled: Neither frames transmitted nor frames received are mirrored.

Both: Frames received and transmitted are mirrored on the Intermediate/Destination port.

Rx only: Frames received on this port are mirrored on the Intermediate/Destination port. Frames transmitted are not mirrored.

Tx only: Frames transmitted on this port are mirrored on the Intermediate/Destination port. Frames received are not mirrored.

| |
|----------|
| Disabled |
| Both |
| Rx only |
| Tx only |

Intermediate

Select the Intermediate port. This checkbox is designed for Remote Mirroring. The Intermediate port is a switched port to connect to the other switch. **Note:** The Intermediate port requires that you disable MAC Table learning (at the **Configuration > MAC Table** menu path).

Destination

Select the Destination port. This checkbox is designed for mirror or Remote Mirroring. The Destination port is a switched port that receives a copy of traffic from the Source port.

Note 1: In Mirror mode, the S4224 only supports one destination port.

Note 2: The destination port requires you to disable MAC Table learning (at the **Configuration > MAC Table** menu path).

Configuration Guideline for All Features

When the switch is running in Remote Mirroring mode, the administrator must check whether other features are enabled or disabled. For example, if MSTP is not disabled on the Reflector port, all monitor traffic will be blocked on the Reflector port.

All recommended settings are as follows:

| | Impact | Source Port | Reflector Port | Intermediate Port | Destination Port | Remote Mirroring VLAN |
|---------------------|---------------|--------------------|-----------------------|--------------------------|-------------------------|------------------------------|
| arp_inspection | High | | * disabled | * disabled | | |
| acl | Critical | | * disabled | * disabled | * disabled | |
| dhcp_relay | High | | * disabled | * disabled | | |
| dhcp_snooping | High | | * disabled | * disabled | | |
| ip_source_guard | Critical | | * disabled | * disabled | * disabled | |
| ipmc/igmpsnp | Critical | | | | | un-conflict |
| ipmc/mldsnp | Critical | | | | | un-conflict |
| lacp | Low | | | o disabled | | |
| lldp | Low | | | o disabled | | |
| mac learning | Critical | | * disabled | * disabled | * disabled | |
| mvr | Critical | | | | | un-conflict |
| nas | Critical | | * authorized | * authorized | * authorized | |
| psec | Critical | | * disabled | * disabled | * disabled | |
| qos | Critical | | * unlimited | * unlimited | * unlimited | |
| upnp | Low | | | o disabled | | |
| mac-based vlan | Critical | | * disabled | * disabled | | |
| protocol-based vlan | Critical | | * disabled | * disabled | | |
| vlan_translation | Critical | | * disabled | * disabled | * disabled | |
| voice_vlan | Critical | | * disabled | * disabled | | |
| mrp | Low | | | | o disabled | |
| mvrp | Low | | | | o disabled | |

Notes:

* -- must

o -- optional

Impact: Critical/High/Low, where:

Critical = 5 packets -> 0 packet

High = 5 packets -> 4 packets

Low = 5 packets -> 6 packets

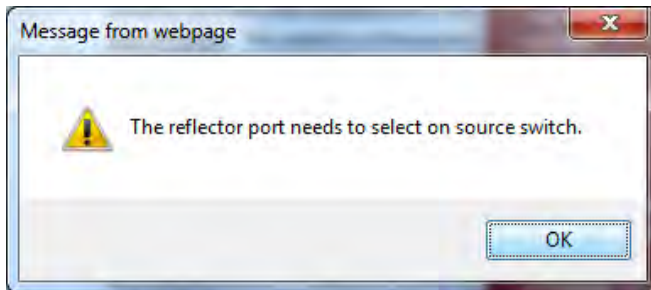
Buttons

Apply: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Messages

Message: *The reflector port needs to select on source switch.*



Meaning: The reflector port requires you to select “Source” as the switch “Type” (see above).

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Select “Source” as the switch “Type” (see above).

PTP Clock Configuration

You can configure S4224 PTP clocking from the **Configuration > PTP** menu path. The Precision Time Protocol (PTP) is a network protocol for synchronizing computer systems' clocks.

Precise time information is especially important for distributed systems in automation technology. With PTP as described in IEEE 1588, it is possible to synchronize distributed clocks to an accuracy of less than 1 microsecond on Ethernet networks. The demands on the local clocks and the network and computing capacity are relatively low.

Two effects are evident when setting or synchronizing clocks: 1) independent clocks initially run at an "offset". To synchronize them, the less accurate clock is set to the more accurate one (offset correction). 2) real clocks do not run at exactly the same speed. Therefore, the speed of the less accurate clock has to be regulated constantly (drift correction).

PTP knows various types of clocks, and acts as a master-to-slave protocol. A clock in an end device is known as an "Ordinary" clock, and a clock in a transmission component like an Ethernet switch is a "Boundary" clock (BC) or "Transparent" clock (TC). A "Master" synchronizes the respective slaves connected to it.

The synchronization process is divided into two phases. First the time difference between the master and the slave is corrected; this is the offset correction. With IEEE1588-2008, two modes are known for the synchronization process: two-step-mode and one-step-mode. The second phase of the synchronization, delay measurement, determines the run time between slave and master. It is determined by the "Delay Request" and "Delay Response" messages in a similar way, and the clocks adjusted accordingly. This can also be done in one-step or in two-step mode. Boundary clocks are required wherever there is a change of the communication technology or other network elements block the propagation of the PTP messages. The IEEE1588-2008 standard knows two types of transparent clocks: End-to-End (E2E) and Peer-to-Peer (P2P). See the IEEE Standards web site at <http://ieeexplore.ieee.org/xpl/standards.jsp> for current editions and amendments.

This page lets you view current PTP clock settings and configure new settings. The default PTP page is shown below. By default, Clock Instance 0 is present. You can configure it separately or along with other PTP clock instances (up to four instances maximum). The default Configuration > **PTP** page:

The screenshot shows the web interface for the S4224 - Carrier Ethernet Network Interface Device. The left sidebar contains a navigation menu with 'Configuration' expanded to show 'PTP'. The main content area is titled 'External I/O Configuration' and includes a table for PTP clock settings, 'External I/O Options' with an impedance dropdown set to 50 Ohms, and a 'PTP Clock Configuration' section with a port list table and buttons for 'Add New PTP Clock', 'Save', and 'Reset'.

External I/O Configuration

| Port | State | Frequency | Actual Frequency |
|------------------|----------|-----------|------------------|
| IEEE 1588 Input | Disabled | 1 PPS | 0 Hz |
| IEEE 1588 Output | Disabled | | - |

External I/O Options

Impedance: 50 Ohms

PTP Clock Configuration

| Delete | Clock Instance | Device Type | Port List | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------------------------|----------------|-------------|-----------|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| No Clock Instances Present | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Buttons: Add New PTP Clock, Save, Reset

Note: at S4224 v 1.0.2, PTP is available over Ethernet and IPv4 only. PTP under IPv6 will be supported at a future release. **Note:** you must have a PTP clock instance configured for accurate RFC 2544 Latency test step timestamps. PTP must be running on both devices to synchronize the Time of Day.

External I/O Configuration

Port

SMB Port and direction (**IEEE 1588 Input** and **IEEE 1588 Output**).

State

Enable or Disable the SMB port. These values are possible:

Enable the port.

Disable the port.

Frequency

Set the Clock Frequency. The following values are possible for input: 1 PPS, 8 KHz, 64 KHz, 1.544 MHz, 2.048 MHz, 10 MHz, 19.44 MHz, or 25 MHz.

The output range is 1-25,000,000 Hz.

For best accuracy, output frequencies should be either:

- 1) A factor of 250,000,000, or
- 2) One of the following special frequencies: 64 KHz, 1.544 MHz, 2.048 MHz.

External I/O Options

Impedance

Select the impedance termination of the port. These values are possible:

50 Ohms: 50 Ohms impedance.

75 Ohms: 75 Ohms impedance.

Hi-Z: no impedance termination driven, "tri-stated" or "floating".

PTP Clock Configuration

Delete

Check this box and click on 'Save' to delete the clock instance.

Clock Instance

Indicates the Instance of a particular Clock Instance [0..3]. Click on the linked Clock Instance number to edit the Clock details for the selected instance.

Device Type

Indicates the Type of the Clock Instance. There are five Device Types.

Ord-Bound - clock's Device Type is Ordinary-Boundary Clock.

P2p Transp - clock's Device Type is Peer to Peer Transparent Clock.

E2e Transp - clock's Device Type is End to End Transparent Clock.

Master Only - clock's Device Type is Master Only.

Slave Only - clock's Device Type is Slave Only.

BC-frontend - clock's Device Type is Boundary Clock frontend.

Port List

Set a check mark for each port configured for this Clock Instance.

2 Step Flag

Static member: defined by system, true if two-step Sync events and Pdelay_Resp events used.

Clock Identity

Shows the unique clock identifier.

One Way

If true, one-way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

Protocol

Transport protocol used by the PTP protocol engine:

ethernet : PTP over Ethernet multicast

ip4multi : PTP over IPv4 multicast

ip4uni : PTP over IPv4 unicast

Note : IPv4 unicast protocol only works in Master only and Slave only clocks . See the 'Device Type' parameter.

In a unicast Slave only clock you must also configure which master clocks to request Announce and Sync messages from. See 'Unicast Slave Configuration'.

VLAN Tag Enable

Enables the VLAN tagging for the PTP frames. **Note**: Packets are only tagged if the port is configured for vlan tagging. i.e: Port Type != Unaware and PortVLAN mode == None, and the port is member of the VLAN.

VID

VLAN Identifier used for tagging the PTP frames.

PCP

Priority Code Point value used for PTP frames.

Buttons

Add New PTP Clock: Click to create a new clock instance.

Save: Click to save the page immediately.

Reset: Click to reset the the page immediately.

From the default **Configuration > PTP** page, click the **Add New PTP Clock** button to display the PTP Clock Configuration table shown below.

| Delete | Clock Instance | Device Type | 2 Step Flag | Clock Identity | One Way | Protocol | VLAN Tag Enable | VID | PCP |
|--------|----------------|-------------|-------------|-------------------------|---------|----------|--------------------------|-----|-----|
| Delete | 1 | Ord-Bound | True | 00:c0:f2:ff:fe:56:16:d1 | False | Ethernet | <input type="checkbox"/> | 1 | 0 |

The PTP Clock Configuration table parameters are described below.

PTP Clock Configuration

The PTP clock configuration parameters are explained below.

Delete

Check this checkbox and click 'Save' to delete an existing clock instance.

Clock Instance

Indicates the Instance of a particular Clock (0-3). Click on the linked Clock Instance number to edit its Clock details.

Device Type

Indicates the Type of the Clock Instance. Select one of the Device Types:

Inactive - no clock type is currently used.

Ord-Bound - clock's Device Type is Ordinary-Boundary Clock.

Select Ord-Bound mode to identify the switch port that is connected to a device with the most precise clock. This is the default clock mode. The device is synchronized with the grand-master clock and operates as a parent master clock. This mode is used for switch ports when overload or heavy load conditions produce significant delay jitter.

P2p Transp - clock's Device Type is Peer to Peer Transparent Clock (TC).

E2e Transp - clock's Device Type is End to End Transparent Clock (BC).

Select E2e Transp mode for the switch to synchronize all switch ports with the grand master clock. The switch corrects for the delay incurred by every packet passing through it (this delay is called 'residence time'). E2e Transp mode causes less jitter and error accumulation than boundary mode.

MastrOnly - clock's Device Type is Master Only.

SlaveOnly - clock's Device Type is Slave Only.

BC-frontend - clock's Device Type is Boundary Clock frontend. The BC frontend mode allows an external CPU to run the PTP protocol and use the switch/PHY to do the timestamping. A frontend port will timestamp Sync packets egressing the port (i.e., update the correction field). Delay request packets ingressing will have the arrival timestamp attached to the packet.

| Device Type |
|-------------|
| Ord-Bound |
| Inactive |
| Ord-Bound |
| P2p Transp |
| E2e Transp |
| Mastronly |
| Slaveonly |
| BC-frontend |

2 Step Flag

Static member: defined by the system, **True** if two-step Sync events and *Pdelay_Resp* events are used, otherwise **False**.

Clock Identity

Displays the unique clock identifier (e.g., 00:c0:f2:ff:fe:56:08:b0).

One Way

If **True**, one way measurements are used. This parameter applies only to a slave. In one way mode, no delay measurements are performed (i.e., this is applicable only if frequency synchronization is needed). The master always responds to delay requests.

Protocol

Select the transport protocol to be used by the PTP protocol engine:

Ethernet PTP over Ethernet multicast.

EtherneMixedt PTP over Ethernet mixed.

IPv4Multi PTP over IPv4 multicast.

IPv4Mixed PTP over IPv4 mixed.

IPv4Uni PTP over IPv4 unicast.

| Protocol |
|---------------|
| Ethernet |
| EthernetMixed |
| IPv4Multi |
| IPv4Mixed |
| IPv4Uni |

Note: The IPv4 unicast protocol only works in Master-only and Slave-only clocks - see the 'Device Type' parameter description.

In a unicast Slave only clock you must also configure which master clocks to request Announce and Sync messages from. See 'Unicast Slave Configuration'.

VLAN Tag Enable

Check to enable the VLAN tagging for the PTP frames. **Note:** Packets are only tagged if the port is configured for VLAN tagging (i.e., Port Type = Unaware and PortVLAN mode = None, and the port is a member of the VLAN).

| VLAN Tag Enable |
|-------------------------------------|
| <input checked="" type="checkbox"/> |

VID

VLAN Identifier used for tagging the PTP frames.

PCP

Priority Code Point value used for PTP frames (0-7).

Buttons

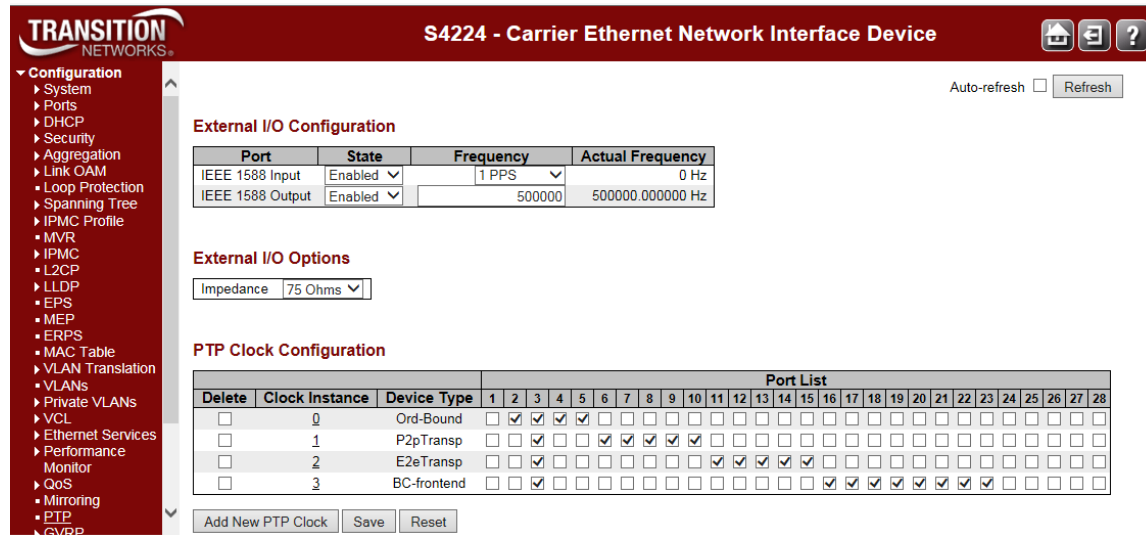
Add New PTP Clock: Click to create a new clock instance. [Up to four clock instances can be created.](#)

Save: Click to save the page immediately. You can add multiple instances with one Save operation.

Reset: Click to reset the page immediately.

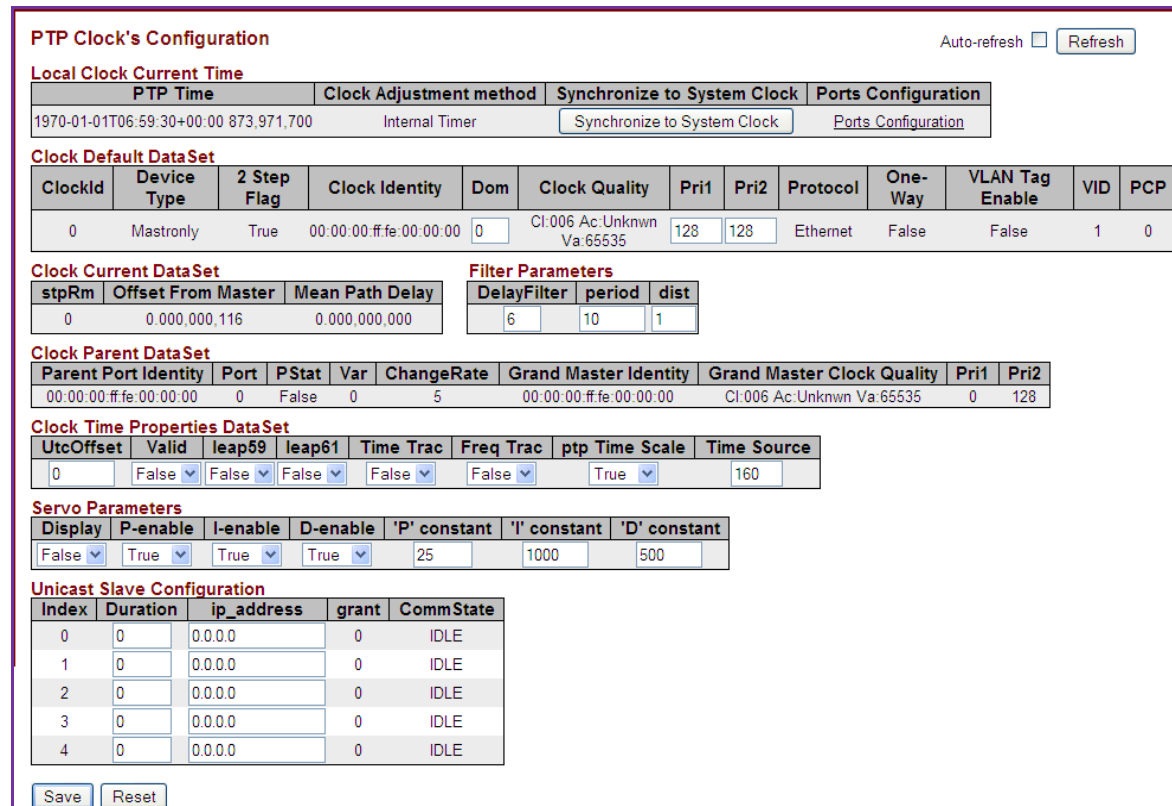
Example

The screen below shows the maximum of four PTP Clock configuration (PTP Clock Instances = 0 to 3).



PTP Clock's Configuration

Click on a linked **Clock Instance** in the PTP Clock Configuration section at the **Configuration > PTP** menu path to display a **PTP Clock's Configuration** page.



Each of the **PTP Clock's Configuration** page sections and fields are explained in the sections below.

Local Clock Current Time table

Local Clock Current Time

| PTP Time | Clock Adjustment method | Synchronize to System Clock | Ports Configuration |
|---------------------------------------|-------------------------|--|-------------------------------------|
| 1970-01-01T06:59:30+00:00 873,971,700 | Internal Timer | <input type="button" value="Synchronize to System Clock"/> | Ports Configuration |

PTP Time

Shows the actual PTP time with nanosecond resolution (e.g., *2012-01-03T19:52:44+00:00 541,523,780*).

Clock Adjustment method

Shows the actual clock adjustment method. The method depends on the available hardware (e.g., Software, Internal Timer, or External Timing (ET) Board).

Internal Timer: uses internal clocking only.

Software: uses software-based clocking only.

hasEtBoardTiming: has an External Timing (RT) Board that is used for timing.

Synchronize to System Clock

You can click the **Synchronize to System Clock** button to synchronize the System Clock to the PTP Time. Select the Clock Type in RFC2544/Y.1564: The delay measurements in RFC2544 and Y.1564 are always done in the IEEE 1588 domain. There is only one timestamping domain which is the 1588. You can synchronize to/from the system time via the Web GUI (at the **Configuration > PTP** menu path) or via the CLI (using the **ptp system-time set** command at the (config) # prompt).

Ports Configuration

Click to edit the port data set for the ports assigned to this clock instance. When you click the [Ports Configuration](#) link, the PTP Clock's Port Data Set Configuration page displays (see below).

Clock Default DataSet table

The clock default data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members defined at clock creation time, the Dynamic members defined by the system, and the configurable members which can be set here.

| Clock Default DataSet | | | | | | | | | | | | |
|-----------------------|-------------|-------------|-------------------------|-----|------------------------------|------|------|----------|---------|-----------------|-----|-----|
| ClockId | Device Type | 2 Step Flag | Clock Identity | Dom | Clock Quality | Pri1 | Pri2 | Protocol | One-Way | VLAN Tag Enable | VID | PCP |
| 0 | Mastronly | True | 00:00:00:ff:fe:00:00:00 | 0 | Cl:006 Ac:Unknwn Va:65535 | 128 | 128 | Ethernet | False | False | 1 | 0 |

ClockId

An internal instance ID (0-3).

Device Type

Indicates the Type of the Clock Instance. The five Device Types are:
ordbound - Clock's Device Type is Ordinary-Boundary Clock.
P2ptransp - Clock's Device Type is Peer to Peer Transparent Clock.
E2etransp - Clock's Device Type is End to End Transparent Clock.
Masteronly - Clock's Device Type is Master Only.
slaveonly - Clock's Device Type is Slave Only.
Bcfrontend - Clock's Device Type is Boundary Clock frontend.

2 Step Flag

Static member: defined by the system, **True** if two-step Sync events and Pdelay_Resp events are used, otherwise **False**.

Clock Identity

Displays the unique clock identifier (e.g., 00:c0:f2:ff:fe:00:00:01).

Dom

The Clock domain (0-127).

Clock Quality

The clock quality is determined by the system, and includes three parts: Clock Class, Clock Accuracy and OffsetScaledLog Variance as defined in IEEE1588 (e.g., Cl:251 Ac:254 Va:65535).

The Clock Accuracy values are defined in IEEE1588 table 6 (the Clock Accuracy is set to **Unknown** by default).

Pri1

Clock priority 1 (0-255) used by the BMC master select algorithm. The Best Master Clock (BMC) algorithm determines which clock is the highest quality clock within the network. The BMC (grandmaster clock) then synchronizes all other (slave) clocks in the network. If the BMC is removed from the network or is found by the BMC algorithm to no longer be the highest quality clock, the algorithm then redefines the new BMC and adjusts all other clocks accordingly. No admin input is needed.

Pri2

Clock priority 2 (0-255) used by the BMC master select algorithm.

Protocol

Transport protocol used by the PTP protocol engine:

Ethernet: PTP over Ethernet multicast

EthernetMixed: PTP using a combination of Ethernet multicast and unicast

IPv4Multi: PTP over IPv4 multicast

IPv4Mixed: PTP using a combination of IPv4 multicast and unicast

IPv4Uni: PTP over IPv4 unicast

One-Way

If **True**, one way measurements are used. This parameter applies only to a slave. In one-way mode, no delay measurements are performed (i.e., this applies only if frequency synchronization is needed). The master always responds to delay requests.

VLAN Tag Enable

The VLAN Tag Enable parameter is ignored, because the tagging is controlled by the VLAN configuration.

VID

The VLAN Identifier used for tagging the VLAN packets.

PCP

The Priority Code Point value used for PTP frames.

Clock Current DataSet table

The **Clock Current DataSet** table displays the current stpRm (e.g., 0) Offset From Master (e.g., 0.000,000,000) and Mean Path Delay (e.g., 0.000,000,000) information. The clock current data set is defined in the IEEE 1588 Standard. The current data set is dynamic.

Clock Current DataSet

| stpRm | Offset From Master | Mean Path Delay |
|-------|--------------------|-----------------|
| 0 | 0.000,000,116 | 0.000,000,000 |

stpRm

Steps Removed: The number of PTP clocks traversed from the grandmaster to the local slave clock.

Offset From Master

The time difference between the master clock and the local slave clock, measured in ns (nanoseconds). A read only value such as 0.000,000,000).

Mean Path Delay

The mean propagation time for the link between the master and the local slave. A read only value such as 0.000,000,000).

Filter Parameters

The **Filter Parameters** table displays the current DelayFilter, Period, and Distance information.

| Filter Parameters | | |
|-------------------|--------|------|
| DelayFilter | period | dist |
| 6 | 10 | 1 |

DelayFilter

The default delay filter is a low pass filter, with a time constant of $2^{**}DelayFilter*DelayRequestRate$. If the DelayFilter parameter is set to 0, the delay filter uses the same algorithm as the offset filter.

period

The default offset filter uses a minimum delay filter method (i.e., the minimum measured offset during Period samples is used in the calculation).

dist

The distance between two calculations is **Dist** periods. **Note:** In configurations with Timestamp enabled PHYs, the period is automatically increased, if $(period*dist < SyncPackets\ pr\ sec/4)$, i.e. max 4 adjustments are made pr sec.

If **dist** is 1 the offset is averaged over the **Period**.

If **dist** is >1 the offset is calculated using 'min' offset.

Clock Parent DataSet table

The **Clock Parent DataSet** is defined in the IEEE 1588 standard. The parent data set is dynamic.

Clock Parent DataSet

| Parent Port Identity | Port | PStat | Var | ChangeRate | Grand Master Identity | Grand Master Clock Quality | Pri1 | Pri2 |
|-------------------------|------|-------|-----|------------|-------------------------|----------------------------|------|------|
| 00:00:00:ff:fe:00:00:00 | 0 | False | 0 | 5 | 00:00:00:ff:fe:00:00:00 | Cl:006 Ac:Unknwn Va:65535 | 0 | 128 |

Parent Port Identity

Clock identity for the parent clock; if the local clock is not a slave, the value is the clocks own ID (e.g., *00:c0:f2:ff:fe:00:00:01*).

Port

The Port ID for the parent master port.

PStat

Parents Stats (always False).

Var

The observed parent offset scaled log variance.

Change Rate

The Observed Parent Clock Phase Change Rate (i.e., the slave clocks rate offset compared to the master). The unit is ns per sec (nanoseconds per second).

Grand Master Identity

The Clock identity for the grand master clock; if the local clock is not a slave, the value is the clock's own ID (e.g., *00:c0:f2:ff:fe:00:00:01*).

Grand Master Clock Quality

The clock quality announced by the grand master, and includes 3 parts: Clock Class, Clock Accuracy and OffsetScaledLog Variance as defined in IEEE1588 (e.g., *Cl:251 Ac:254 Va:65535*). The Clock Accuracy values are defined in IEEE1588 - Table 6 (the clock Accuracy is currently set to **Unknown** as the default).

Pri1

Clock priority 1 announced by the grand master.

Pri2

Clock priority 2 announced by the grand master.

Clock Time Properties DataSet

The clock time properties data set is defined in the IEEE 1588 Standard. The data set is both configurable and dynamic (i.e., the parameters can be configured for a grandmaster). In a slave clock, the parameters are overwritten by the grandmasters timing properties. The parameters are not used in the current PTP implementation.

Clock Time Properties DataSet

| UtcOffset | Valid | leap59 | leap61 | Time Trac | Freq Trac | ptp Time Scale | Time Source |
|-----------|-------|--------|--------|-----------|-----------|----------------|-------------|
| 0 | False | False | False | False | False | True | 160 |

UtcOffset

The current UtcOffset (e.g., 0). The UTC offset is the time offset from Coordinated Universal Time (UTC). It is typically given as hour or hour and minute. Many time zones employ two time offsets; one for standard time and one for daylight saving time.

Valid

The current Valid setting (**True** or **False**).

leap59

The current leap59 setting (**True** or **False**).

leap61

The current leap61 setting (**True** or **False**).

Time Trac

The current Time Trac setting (**True** or **False**).

Freq Trac

The current Freq Trac setting (**True** or **False**).

ptp Time Scale

The current ptp Time Scale setting (**True** or **False**).

Time Source

The valid values for the Time Source parameter are:

- 16 (0x10) ATOMIC_CLOCK
- 32 (0x20) GPS
- 48 (0x30) TERRESTRIAL_RADIO
- 64 (0x40) PTP
- 80 (0x50) NTP
- 96 (0x60) HAND_SET
- 144 (0x90) OTHER
- 160 (0xA0) INTERNAL_OSCILLATOR (the default setting)

Messages:

External Clock feature not present

External PPS feature not present

Servo Parameters

The default clock servo uses a PID regulator to calculate the current clock rate using the formula:

clockAdjustment = OffsetFromMaster/ P constant + Integral(OffsetFromMaster)/ I constant + Differential OffsetFromMaster/ D constant

A Proportional - Integral - Derivative controller (PID controller) is a control loop feedback mechanism widely used in industrial control systems. A PID is a commonly used type of feedback controller. A PID controller calculates an "error" value as the difference between a measured process variable and a desired setpoint. The PID controller tries to minimize the error by adjusting the process control inputs.

The PID controller calculation involves three separate constant parameters: the Proportional, the Integral, and the Derivative values (**P**, **I**, and **D**). These values can be interpreted in terms of time, where:

P depends on the present error,

I depends on the accumulation of past errors, and

D is a prediction of future errors, based on current rate of change.

The weighted sum of these three actions is used to adjust the process via a control element such as the position of a valve, or the amount of power supplied to a heating element. The Proportional, Integral, and Derivative terms are summed to calculate the output of the PID controller.

By tuning these three parameters in the PID controller algorithm, the controller can provide control action designed for specific process requirements.

Servo Parameters

| Display | P-enable | I-enable | D-enable | 'P' constant | 'I' constant | 'D' constant |
|---------|----------|----------|----------|--------------|--------------|--------------|
| False | True | True | True | 25 | 1000 | 500 |

The Servo Parameters are explained below.

Display

If **True** then *Offset From Master*, *MeanPathDelay* and *clockAdjustment* are logged on the debug terminal.

P-enable

If **True** the **P** part of the algorithm (**Proportional**) is included in the calculation.

I-Enable

If **True** the **I** part of the algorithm (**Integral**) is included in the calculation.

D-enable

If **True** the **D** part of the algorithm (**Derivative**) is included in the calculation.

'P' constant

The **Proportional** value [1-1000]. The **Proportional** value makes a change to the output that is proportional to the current error value.

'I' constant

The **Integral** value [1-10000]. The **Integral** is the sum of the instantaneous error over time and gives the accumulated offset that should have been corrected previously.

'D' constant

The **Derivative** value [1-10000]. The **Derivative** of the process error is calculated by determining the slope of the error over time and multiplying this rate of change by the derivative gain. The derivative term slows the rate of change of the controller output.

Unicast Slave Configuration

When operating in IPv4 Unicast mode, the slave is configured up to five master IP addresses. The slave then requests *Announce* messages from all the configured masters. The slave uses the BMC algorithm to select one as the master clock; the slave then requests *Sync* messages from the selected master.

Unicast Slave Configuration

| Index | Duration | ip_address | grant | CommState |
|-------|----------|------------|-------|-----------|
| 0 | 0 | 0.0.0.0 | 0 | IDLE |
| 1 | 0 | 0.0.0.0 | 0 | IDLE |
| 2 | 0 | 0.0.0.0 | 0 | IDLE |
| 3 | 0 | 0.0.0.0 | 0 | IDLE |
| 4 | 0 | 0.0.0.0 | 0 | IDLE |

Duration

The number of seconds a master is requested to send Announce/Sync messages. The request is repeated from the slave each Duration/4 seconds.

ip_address

The IPv4 Address of the Master clock.

grant

The granted repetition period for the sync message.

CommState

The state of the communication with the master, possible values are:

IDLE : The entry is not in use.

INIT : Announce is sent to the master (Waiting for a response).

CONN : The master has responded.

SELL : The assigned master is selected as current master.

SYNC : The master is sending Sync messages.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

PTP Clock's Port Data Set Configuration

Click on the [Ports Configuration Page](#) link in the PTP Clock's Configuration section to display the **PTP Clock's Port Data Set Configuration** table. The port data set is defined in the IEEE 1588 Standard. It has three groups of data: the static members, the dynamic members, and configurable members which can be set here.

The ports displayed here are the ports enable (checkboxes checked) at the PTP Clock Configuration table in the Port List column (e.g., Ports 4-8, and 19-22 in the sample screen below).

| Port | Stat | MDR | PeerMeanPathDel | Anv | ATo | Syv | DIm | MPR | Delay Asymmetry | Ingress Latency | Egress Latency | Version |
|------|------|-----|-----------------|-----|-----|-----|-----|-----|-----------------|-----------------|----------------|---------|
| 4 | dsbl | 0 | 0.000,000,000 | 1 | 3 | 0 | e2e | 3 | 0 | 0 | 0 | 2 |
| 5 | dsbl | 0 | 0.000,000,000 | 1 | 3 | 0 | e2e | 3 | 0 | 0 | 0 | 2 |
| 6 | dsbl | 0 | 0.000,000,000 | 1 | 3 | 0 | e2e | 3 | 0 | 0 | 0 | 2 |
| 7 | dsbl | 0 | 0.000,000,000 | 1 | 3 | 0 | e2e | 3 | 0 | 0 | 0 | 2 |
| 8 | dsbl | 0 | 0.000,000,000 | 1 | 3 | 0 | e2e | 3 | 0 | 0 | 0 | 2 |
| 19 | dsbl | 0 | 0.000,000,000 | 1 | 3 | 0 | e2e | 3 | 0 | 0 | 0 | 2 |
| 20 | dsbl | 0 | 0.000,000,000 | 1 | 3 | 0 | e2e | 3 | 0 | 0 | 0 | 2 |
| 21 | dsbl | 0 | 0.000,000,000 | 1 | 3 | 0 | e2e | 3 | 0 | 0 | 0 | 2 |
| 22 | dsbl | 0 | 0.000,000,000 | 1 | 3 | 0 | e2e | 3 | 0 | 0 | 0 | 2 |

The related **The PTP Clock's Port Data Set Configuration** table parameters are explained below.

Port

Static member port Identity: Port number (2-6). This is the S4224 port number. Note that PTP configuration of the S4224 MGMT port is not supported.

Stat

Dynamic member *portState*: the current state of the port. The clock's port status (e.g., **dsbl** or **p2pt**).

MDR

Dynamic member log *Min Delay Req Interval*: The delay request interval announced by the master (e.g., **0** or **3**).

Peer Mean Path Del

The path delay measured by the port in P2P mode. In E2E mode this value is **0** (e.g., **0.000,000,000**).

Anv

The interval for issuing announce messages in master state (e.g., **1**). The valid range is **-3** to **4**.

ATo

The timeout for receiving announce messages on the port (e.g., **3**). The valid range is **-1** to **10**.

Syv

The interval for issuing sync messages in the master (e.g., **0**). The Sync Interval must be an integer value between **-7** and **4**.

Dlm

Configurable member *delayMechanism*: the delay mechanism used for the port (e.g., **p2pt** for Peer to Peer Transparent), where:

e2e: End to end delay measurement.

p2p: Peer to peer delay measurement.

dsb1: Delay is disabled.

Dlm can be defined per port in an Ordinary/Boundary clock. In a transparent clock, all ports use the same delay mechanism, as determined by the clock type.

MPR

The interval for issuing *Delay_Req* messages for the port in E2e mode. This value is announced from the master to the slave in an announce message. The value is reflected in the MDR field in the Slave. This is the interval for issuing *Pdelay_Req* messages for the port in P2P mode.

The valid range is **-7** to **5**.

Note: The interpretation of this parameter has changed from v 1.2 to v 2.0. In earlier versions the value was interpreted relative to the Sync interval; this was a violation of the standard, so now the value is interpreted as an interval (i.e., MPR = 0 => 1 Delay_Req pr sec, independent of the Sync rate).

Delay Asymmetry

If the transmission delay for a link is not symmetric, the asymmetry can be configured here (e.g., *0.000,000,000*). See IEEE 1588 Section 7.4.2 Communication path asymmetry.

The valid range is **-1000000** to **1000000**.

Ingress Latency

Ingress latency measured in ns (nanoseconds), as defined in IEEE 1588 Section 7.3.4.2.

The valid range is **-1000000** to **1000000**.

Egress Latency

Egress latency measured in ns (nanoseconds), as defined in IEEE 1588 Section 7.3.4.2.

The valid range is **-1000000** to **1000000**.

Version

The current implementation supports PTP version **2** (e.g., version 2) only.

Buttons

Save : Click to save changes.

Reset : Click to undo any changes made locally and revert to previously saved values.

GVRP Configuration

You can configure S4224 GVRP globally and at the port level from the **Configuration > GVRP** menu path. Generic VLAN Registration (GVRP) is specified in IEEE 802.1Q-2005 clause 11 and IEEE 802.1D Clause 12. A small number of GVRP parameters can be configured.

GVRP (GARP VLAN Registration Protocol) allows network devices to share VLAN information and to use the information to modify existing VLANs or create new VLANs, automatically. This makes it easier to manage VLANs that span more than one switch. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices. See the IEEE standards page at <http://standards.ieee.org/findstds/standard/802.1D-2004.html>. See the Global VLAN and Port VLAN configuration section for related information.

GVRP Global Configuration

GVRP is enabled globally (at the device level) from **Configuration > GVRP > Global config**.

The screenshot shows the GVRP Configuration page. The title bar reads "S4224 - Carrier Ethernet Network Interface Device". The main content area is titled "GVRP Configuration" and includes a "Refresh" button. Below the title is a checkbox labeled "Enable GVRP". Underneath is a table with the following parameters and values:

| Parameter | Value |
|----------------|-------|
| Join-time: | 20 |
| Leave-time: | 60 |
| LeaveAll-time: | 1000 |
| Max VLANs: | 20 |

At the bottom of the configuration area is a "Save" button.

Enable GVRP (Global) Checkbox

Use the checkbox to enable GVRP globally. GVRP is fully enabled only when GVRP is globally enabled and enabled on the specific port(s) and saved. The default is GVRP disabled (unchecked).

Join-time

The default is **20** centiseconds (hundredths of a second). Join-time is a value in the range **1-20** in the units of centi seconds (i.e., in units of one hundredth of a second). The default is **20**.

Leave-time

Leave-time is a value in the range **60-300** in the units of centi seconds (one hundredths of a second). The default is **60** centiseconds.

LeaveAll-time

LeaveAll-time is a value in the range **1000-5000** in the units of centi seconds (one hundredths of a second). The default is **1000** centiseconds (hundredths of a second).

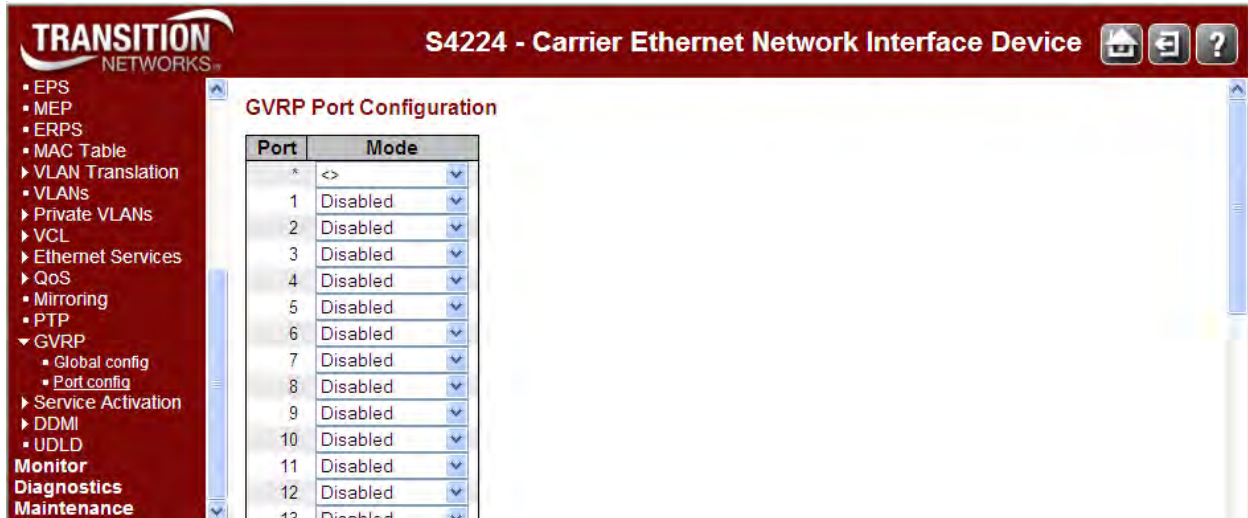
Max VLANs

When GVRP is enabled, a maximum number of VLANs supported by GVRP is specified. By default this number is **20**. This number can only be changed when GVRP is (temporarily) disabled at the Enable GVRP checkbox (see above).

GVRP Port Configuration

The **Configuration > GVRP > Port config** menu path lets you to enable one or more ports for GVRP.

This configuration can be performed either before or after GVRP is configured globally - the protocol operation will be the same. Note that GVRP must be enabled both globally and at the port level to work.



The GVRP Port Configuration parameters are described below.

Port

The logical port that is to be configured.

Mode

Enable or disable GVRP for each specific port. These values turn the GVRP feature off or on respectively for the port in question.

GVRP Enabled: enable GVRP at the port level.

Disabled: disable GVRP at the port level.

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Service Activation Configuration

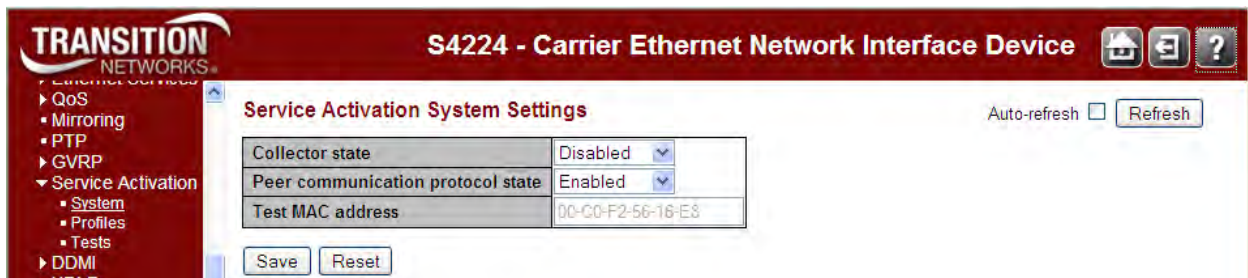
The **Configuration > Service Activation** menu path lets you configure Service Activation System Settings, Profiles, and Tests.



Service Activation Configuration

Configuration > Service Activation > System

Navigate to the **Configuration > Service Activation > System** menu path to display the Service Activation (SA) System Settings.



The settings are described below.

Collector state

The Collector Flag enables or disables the SA module's ability to accept SA test requests from outside. The default is Disabled. The Collector Flag determines if the SA module accept SA test requests from outside.

Peer communication protocol state

Enable/disable the peer communication protocol. If this attribute is disabled, a NID is unable to support unidirectional and bidirectional RFC2544 tests (both as Initiator and Collector) since it cannot communicate with the far end. Only loopback tests can be executed in this case.

Test MAC address

. The Test MAC Address is used as the source MAC address of the generating frames.

Buttons

Auto-refresh: Check this box to refresh the page automatically every three seconds.

Refresh: Click to refresh the page; any changes made locally will be undone.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Configuration > Service Activation > Profiles

Navigate to the **Configuration > Service Activation > Profiles** menu path to display the default Service Activation Profiles Configuration page. Click the **Add New Profile** button to display the configurable parameters.

Service Activation Profiles Configuration

Profile ID

The profile entry ID.

Name

The name of the profile.

Payload Fill

Payload filler (**PRBS** or **Fixed**). PRBS (pseudorandom bit sequence) is a highly random sequence with no correlation between adjacent bits.

Payload Fill Pattern (hex)

The Payload Fill Pattern (in hexadecimal).

CBS Line Rate (Mbps)

Line rate at which burst traffic should be sent for the Back-to-back frames test. In Mbps.

FLR (%)

Acceptable frame loss ratio (expressed in percentage, with 2 decimals (i.e. 99.99 %)).

Yellow Frames PCP Values

List of PCP values corresponding to yellow frame (0-7).

Frame Size Mix (bytes)

Traffic frame size mix, for throughput tests (64-10056, with no two values the same, in multiples of 4).

Rate Decrease Step (%)

Rate decrease step size, in percentage. The valid range is 10-90%.

Step Length (sec)

Rate step length, in seconds. The valid range is 10-300 seconds.

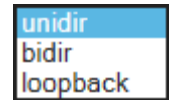
Test Mode

The test direction or type: **uni-directional**, **bi-directional** or **loopback**.

unidirectional: enables uni-directional test mode.

bidirectional: enables bi-directional test mode.

loopback: enables loopback test mode. Set both sides to **loopback**.

**Test steps**

List of tests to execute (**Throughput**, **Latency**, **Frame Loss Rate**, and/or **Back-to-Back**). Check one or more of the tests to run.

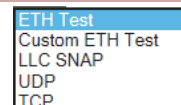
Encapsulation Level

Frame level (e.g., **L2** or **L3**). The Encapsulation Level and the Encapsulation Type must correspond. For example, Encapsulation Level **L3** corresponds to Encapsulation Types **UDP** and **TCP**.

Encapsulation Type

Encapsulation type for L2/L3 frames (**ETH Test**, **Custom ETH Test**, **LLC SNAP**, **UDP**, or **TCP**).

The minimum frame size for TCP encapsulation is 68 bytes.

**Custom Eth Type (hex)**

Custom Eth-Type for L2 ETH-TST frames in hexadecimal (e.g., **8902**).

MEG Level

Level of MEG that is used by ETH-TST frames (0-7).

LLC/SNAP OUI (hex)

LLC/SNAP OUI field (3 bytes). The valid range is 0-65535.

LLC/SNAP Protocol

LLC/SNAP protocol field (0-65535).

Dest IP

The Destination IP address. Enter a valid IP address in dotted decimal notation (x.y.z.w), with these restrictions:

- 1) x, y, z, and w must be decimal numbers from 0-255,
- 2) x must not be 0 unless x, y, and w are also 0,
- 3) x must not be 127, and
- 4) x must not be greater than 223.

Src IP

The Source IP address. Enter a valid IP address in dotted decimal notation (x.y.z.w), with these restrictions:

- 1) x, y, z, and w must be decimal numbers from 0-255,
- 2) x must not be 0 unless x, y, and w are also 0,
- 3) x must not be 127, and
- 4) x must not be greater than 223.

DSCP (hex)

DSCP value for L3 IP frames. The valid range is 0-3f.

ECN

ECN value for L3 IP frames. The valid range is 0-3.

Flags

Flags value for L3 IP frames. The valid range is 0-7.

TTL

TTL (Time To Live) value for L3 IP frames. The valid range is 0-255.

Src Port

Source port for L3 TCP or UDP frames. The valid range is 0-65535.

Dest Port

Destination port for L3 TCP or UDP frames. The valid range is 0-65535.

Seq Number

Sequence number for L3 IP/TCP frames. The valid range is 0-4294967295.

ACK

ACK number for L3 IP/TCP frames. The valid range is 0-4294967295.

Control Bits (hex)

Control bits for L3 IP/TCP frames. The valid range is 0-3f.

Window Size

Window size for L3 IP/TCP frames. The valid range is 0-65535.

DM Threshold Configuration

Delay Measurement threshold values in usec. DM Threshold must be sorted and last value must be 5000000.

| DM Threshold Configuration | | | |
|----------------------------|----|---------|------|
| 0 | to | 5000000 | usec |
| 5000001 | to | 5000001 | usec |
| 5000002 | to | 5000002 | usec |
| 5000003 | to | 5000003 | usec |
| 0 | to | 0 | usec |

DMV Threshold Configuration

Delay Measurement Variation threshold values in usec. DMV Threshold must be sorted and last value must be 5000000.

| DMV Threshold Configuration | | | |
|-----------------------------|----|---------|------|
| 0 | to | 5000000 | usec |
| 5000001 | to | 5000001 | usec |
| 5000002 | to | 5000002 | usec |
| 5000003 | to | 5000003 | usec |
| 0 | to | 0 | usec |

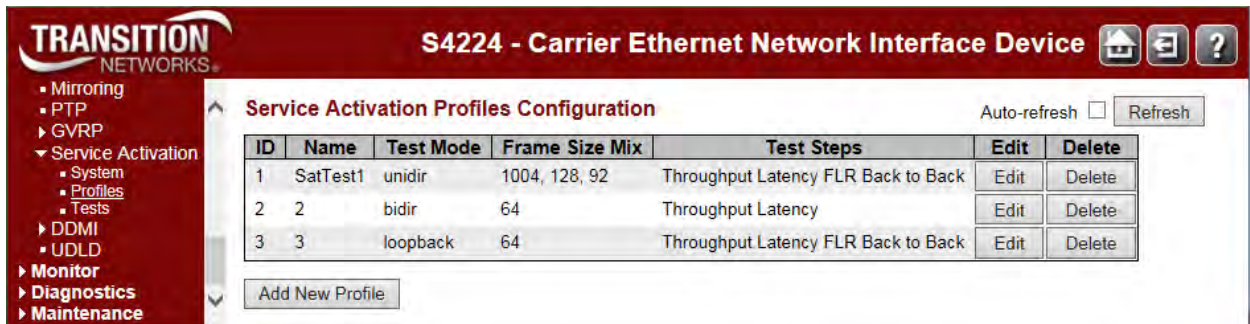
Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Example

One Service Activation Profile configured for each available Test Mode:



Configuration > Service Activation > Tests

Navigate to the **Configuration > Service Activation > Tests** menu path to display the default Service Activation Tests Configuration page. Click the **Add New Test** button to display the configurable parameters. See also [Diagnostics > Service Activation](#) on page 528.

Service Activation Tests Configuration

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

Service Activation Tests Configuration

| Test settings | |
|--------------------------|-------------------|
| ID | 1 |
| Name | |
| Profile | |
| Collector IP | 0.0.0.0 |
| Target MAC address | 00-00-00-00-00-00 |
| Ingress Port | 1 |
| Collector's Ingress Port | 1 |
| Egress Port | 1 |
| EVC/ECE | 0/0 |

| Ingress Tag configuration | |
|---------------------------|----------|
| Encapsulation | Untagged |
| Inner VID | 0 |
| Inner PCP | 0 |
| Outer VID | 0 |
| Outer PCP | 0 |

| Egress Tag configuration | |
|--------------------------|----------|
| Encapsulation | Untagged |
| Inner VID | 0 |
| Inner PCP | 0 |
| Outer VID | 0 |
| Outer PCP | 0 |

| Bandwidth configuration | |
|-------------------------|---|
| CIR (bps) | 500000000 |
| CBS (bytes) | 1000000 |
| EIR (bps) | 0 |
| EBS (bytes) | 0 |
| Policer to import from | 1 <input type="button" value="Import"/> |

Test settings

ID

The test entry ID.

Name

The Test name. Do not use special characters (**#\$%^&*()**) in the Test Name.

Profile

The SA profile for the test.

Collector IP

IP address of the collector.

Target MAC address

The Target Test MAC address (to be used for Loopback test only). The EtherSAT Test MAC address (48 bit MAC address in the format **xx:xx:xx:xx:xx:xx**).

Ingress Port

The Ingress port number.

Collector's Ingress Port

Collector's ingress port number.

Egress Port

The Egress port number.

EVC/ECE

The EVC and ECE associated with test (e.g., 1/1).

Ingress Tag configuration**Ingress Tag Encapsulation**

VLAN tag encapsulation type (**Untagged**, **C-tag**, **S-tag**, **CC-tag**, or **SC-tag**).

| Encapsulation | Untagged |
|---------------|----------|
| | C-tag |
| | S-tag |
| | CC-tag |
| | SC-tag |

Ingress Tag Inner VID

Ingress Inner VLAN ID (0-4095).

Ingress Tag Inner PCP

Ingress Inner PCP value (0-7).

Ingress Tag Outer VID

Ingress Outer VLAN ID (0-4095).

Ingress Tag Outer PCP

Ingress Outer PCP value (0-7).

Egress Tag configuration**Egress Tag Encapsulation**

VLAN tag encapsulation type (**Untagged**, **C-tag**, **S-tag**, **CC-tag**, or **SC-tag**).

| Encapsulation | Untagged |
|---------------|----------|
| | C-tag |
| | S-tag |
| | CC-tag |
| | SC-tag |

Egress Tag Inner VID

The Egress Inner VLAN ID (0-4095).

Egress Tag Inner PCP

The Egress Inner PCP value (0-7).

Egress Tag Outer VID

The Egress Outer VLAN ID (0-4095).

Egress Tag Outer PCP

The Egress Outer PCP value (0-7).

Bandwidth configuration

CIR (bps)

The Committed Information Rate in bps. The average bandwidth for a virtual circuit guaranteed to work under normal conditions.

CBS (bytes)

The Committed Burst Rate in bytes.

EIR (bps)

The Excess Information Rate in bps.

EBS (bytes)

The Excess Busrt Size In bytes (0-100000 bytes).

Policer to import from

The Policer (1-128) to imports bandwidth settings from.

Buttons

Import: Imports bandwidth settings from selected policer (1-128).

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Messages

Message: *Error: tn_ether_sat_lb_conf_set failed*

Meaning: The Factory Defaults web command does not reset Service Actation Loopback. After the Factory Defaults web command successfully completes, the Service Activation Loopback is still active. However, the shared port has been reset to external and at this point the loopback can not be set to inactive. When attempted, the following error is reported on the CLI:

E web 01:42:26 76/handler_config_tn_ether_sat#126: Error: tn_ether_sat_lb_conf_set failed

Recovery: To deactivate the loopback, set the shared port back to internal.

DDMI Configuration

The **Configuration > DDMI** menu path lets you configure general DDMI and DDMI mode parameters.

DDMI (Digital Diagnostics Monitoring Interface) provides an enhanced digital diagnostic monitoring interface for optical transceivers which allows real time access to device operating parameters.

Configuration > DDMI > General

Here you enable or disable DDMI global operation.



Mode

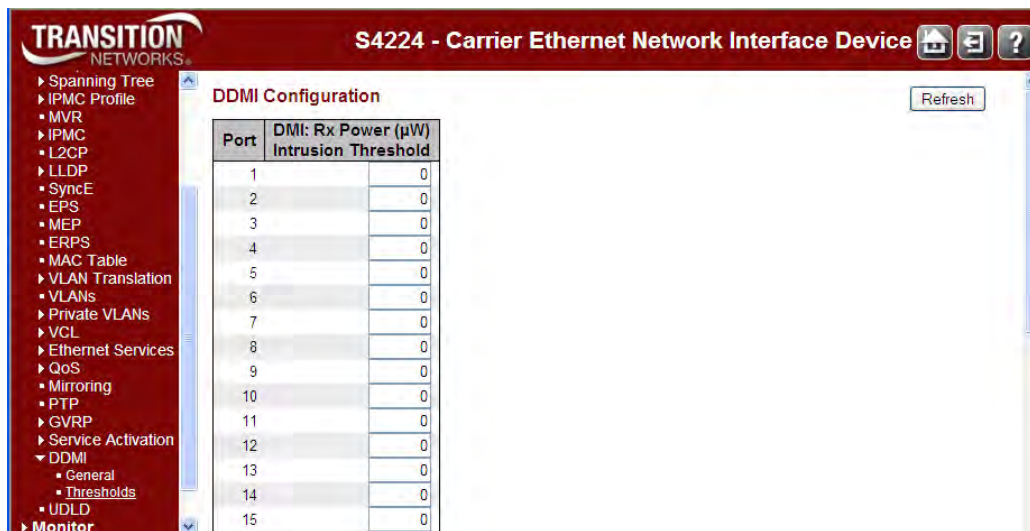
Sets / indicates the DDMI mode of operation. Possible modes are:

Enabled: Enable DDMI mode operation.

Disabled: Disable DDMI mode operation (default).

Configuration > DDMI > Thresholds

Here you configure DDMI at the port level.



Port

This is the logical port number for this row.

DMI: Rx Power (uW) Intrusion Threshold

A level for Rx Power on the Fiber port. If the DMI read value falls below the preset value, an intrusion is detected, and a trap is generated. The default is 0 uW. The range is 0 - 65,535 uW.

Buttons

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

UDLD Configuration

The UDLD Port Configuration page lets you view and configure the current UDLD (Uni Directional Link Detection) from the **Configuration > UDLD** menu path.

The UDLD protocol monitors the physical configuration of the links between devices and ports that support UDLD. It detects the existence of unidirectional links. UDLD is used to provide mechanisms useful for detecting one way connections before they create a loop or other protocol malfunction. IETF [RFC 5171](#) specifies a way at the Data link layer to detect a Uni-directional link.

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

UDLD Port Configuration

| Port | UDLD mode | Message Interval |
|------|-----------|------------------|
| * | <> | 7 |
| 1 | Disable | 7 |
| 2 | Disable | 7 |
| 3 | Disable | 7 |
| 4 | Disable | 7 |
| 5 | Disable | 7 |
| 6 | Disable | 7 |
| 7 | Disable | 7 |
| 8 | Disable | 7 |
| 9 | Disable | 7 |
| 10 | Disable | 7 |
| 11 | Disable | 7 |
| 12 | Disable | 7 |
| 13 | Disable | 7 |
| 14 | Disable | 7 |
| 15 | Disable | 7 |
| 16 | Disable | 7 |
| 17 | Disable | 7 |
| 18 | Disable | 7 |
| 19 | Disable | 7 |
| 20 | Disable | 7 |

Port

The Port number configured by this row.

UDLD mode

Configures the UDLD mode on a port. Valid values are Disable, Normal and Aggressive. The default mode is **Disabled**.

Disable: In disabled mode, UDLD functionality doesn't exist on port.

Normal: In normal mode, if the link state of the port was determined to be uni-directional, it will not affect the port state.

Aggressive: In aggressive mode, Uni-directional detected ports will get shutdown. To bring back the ports up, you must disable UDLD on that port.

Message Interval

Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from **7** to **90** seconds. (The default value is **7** seconds; currently the default time interval is supported due to lack of detailed information in RFC 5171).

Buttons

Save: Click to save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

Monitor Main Menu

- ▼ **Monitor**
 - ▶ System
 - ▶ **Ports**
 - ▶ Link OAM
 - ▶ DHCP
 - ▶ Security
 - ▶ LACP
 - Loop Protection
 - ▶ Spanning Tree
 - ▶ MVR
 - ▶ IPMC
 - ▶ LLDP
 - ▶ Ethernet Services
 - PTP
 - MAC Table
 - ▶ VLANs
 - ▶ DDMI
 - UDLD

The **Monitor** main menu lets you view and track S4224 operating functions.

(The related operating functions are defined at the **Configuration** main menu path.)

Each of the Monitor sub-menu functions is described below.

Monitor > System > Information

S4224 system information is displayed at the **Monitor > System > Information** menu path. (System information is entered from the **Configuration > System > Information** menu path.)

| System | | |
|------------------|---------------------------|------|
| Contact | | |
| Name | | |
| Location | | |
| Hardware | | |
| Product ID | S4224 | |
| Serial # | 3012 | |
| Board Rev | 3 | |
| FPGA Version | v2.3 | |
| Board Temp | 36 C | |
| CPU Temp | 45 C | |
| MAC Address | 00-c0-e2-56-16-d0 | |
| Chip ID | VSC7460 Rev. B | |
| Time | | |
| System Date | 1970-01-01T05:11:50+00:00 | |
| System Uptime | 0d 05:11:50 | |
| Software | | |
| Software Version | S4224 (standalone) 2.2.0 | |
| Software Date | 2015-07-13T22:12:58-05:00 | |
| Acknowledgments | Details | |
| Power Supplies | | |
| | PS 1 | PS 2 |
| Present | Yes | Yes |
| Powered | Yes | No |
| Type | AC | DC |
| Fan RPM | 4651 | 4573 |
| Temperature | 27 C | 26 C |

The system information parameters are explained below.

Contact

Displays the system contact configured at **Configuration > System > Information > System Contact**.

Name

Displays the system name configured at **Configuration > System > Information > System Name**.

Location

The system location configured at **Configuration > System > Information > System Location**.

Product ID

A specific product identifier (S4224).

Serial #

The S4224 device's unique serial number (e.g., # 3012).

Board Rev

The revision of the S4224 PCB (printed circuit board) (e.g., 3).

FPGA Version

The current version of the FPGA (field programmable gate array) (e.g., v2.3).

Board Temp

The PCB temperature in degrees C.

CPU Temp

The processor temperature in degrees C.

MAC Address

Displays the MAC Address of this S4224 (e.g., 00-c0-f2-56-08-b0).

Chip ID

The Chip ID of this S4224 (e.g., VSC7460 Rev. B).

System Date

The current (GMT) system time and date (e.g., 1970-01-01T19:05:44+00:00). The system time is obtained through the configured timing server, if any is configured.

System Uptime

The period of time the device has been operational (e.g., 4d 19:05:44).

Software Version

The software version of this S4224 (e.g., S4224 (standalone) 2.2.0).

Software Date

The date and time when the S4224 software was produced (e.g., 2015-07-14T22:12:23-05:00).

Acknowledgements

Click the [Details](#) link to display the related open source components. See [Appendix B - Licenses](#) on page 601.

Power Supplies

Whether Power Supplies PS 1 and/or PS 2 are Present (Yes or No), Powered (Yes or No), the Type (AC or DC), the Fan RPM (e.g., 4643 or 4576 RPMs), and the PS1 and/or PS2 Temperature (e.g., 26° C / 25 °C).

Buttons

Auto-refresh: Check this checkbox to automatically refresh the page every three seconds.

Refresh: Click to refresh the page; any changes made locally will be undone.

Monitor > System > CPU Load

This page displays the CPU load, using an SVG graph. The load is measured as averaged over the last 100 milliseconds, 1 second and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well.

By default displays “Microsoft Internet Explorer needs the [Adobe SVG Plugin](#) to display this page.”



Your browser must support the SVG format in order to display the SVG graph. Consult the [SVG Wiki](#) for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer must have a plugin installed to support SVG.

Download Adobe® SVG Viewer 3 for data-driven, interactive SVG graphics on the web. Read the [Release Notes](#) and support documentation for important information about this release. Note that Adobe [announced](#) discontinued support for Adobe SVG Viewer on January 1, 2009.

Scalable Vector Graphics (SVG) is a set of specifications for an XML-based file format for describing two-dimensional vector graphics, both static (interactive) and dynamic (animated). The SVG specification is an open standard that has been under development by the W3C since 1999. SVG images and their behaviors are defined in XML text files. This means that they can be searched, indexed, scripted and, if required, compressed. All major modern web browsers have at least some degree of SVG support, and can render SVG markup directly, including Mozilla Firefox, Internet Explorer 9, Google Chrome, Opera, and Safari. However, versions of Microsoft Internet Explorer before IE9 support SVG natively.

To download, install and run the Adobe SVG Plugin

If you want to download, install, and run the plugin, perform the steps below. (As an alternative, you can just run the plugin without downloading/installing, as explained in the next section.)

1. Click the [Adobe SVG Plugin](#) link. A new window opens with the Adobe SVG Viewer download area.
2. To install the Adobe SVG Viewer, double-click the downloaded installer and follow the on-screen instructions.
3. Click **Save** at the prompt. Click **Run** to run the program. (You must have Admin privileges on your computer.)

If you are not using Internet Explorer, you must restart your browser before viewing SVG.

To run the Adobe SVG Plugin:

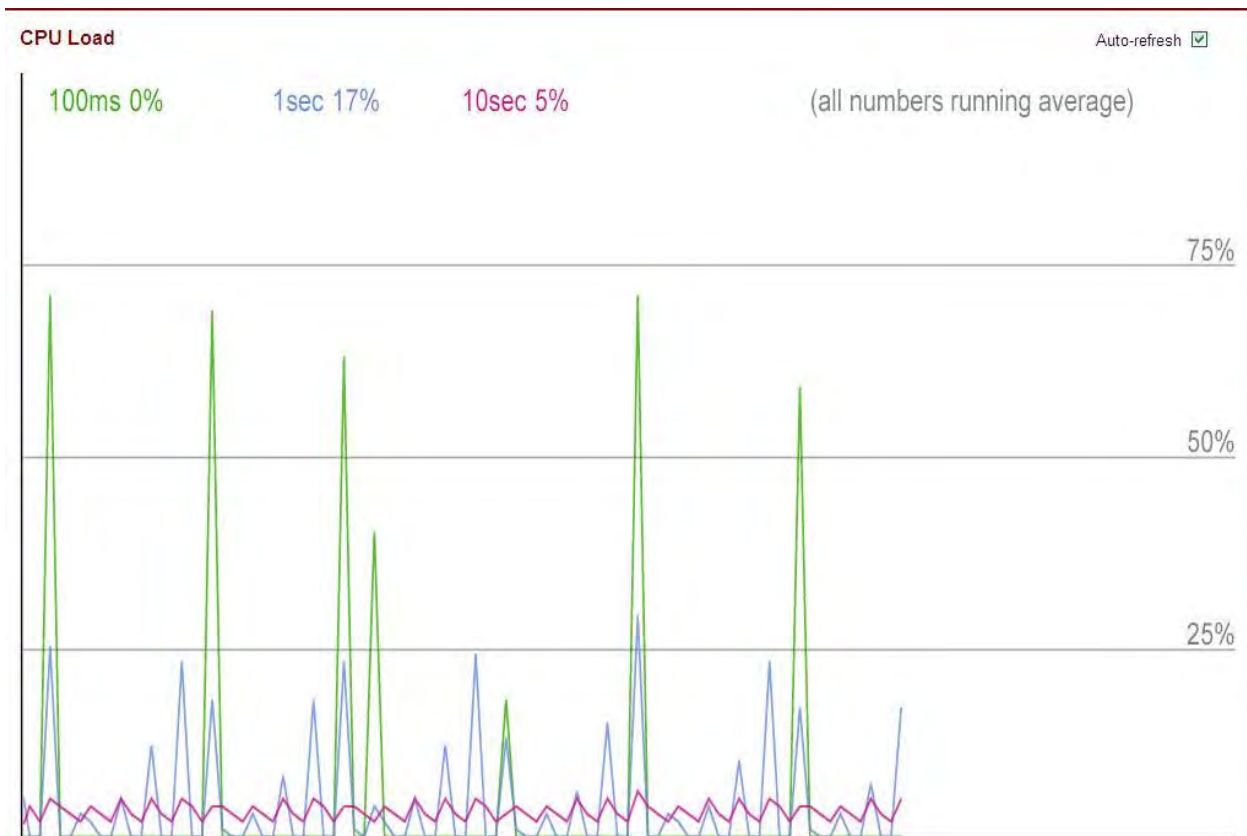
If you want to run the plugin without installing it, perform the steps below.

At the information / message bar above the S4224 web page, click “*This website wants to run the following add-on: ‘SVG Viewer 3.0.2 for Netscape’ from ‘Adobe Systems, Inc.’ (unverified publisher). If you trust the website and the add-on, and want to allow it to run, click here ...*”

The CPU Load page displays using an SVG graph. The message “*Collecting data, please wait ...*” displays momentarily, and then some initial CPU load data displays.

The load is measured as averaged over the last 100 milliseconds, 1 second and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well.

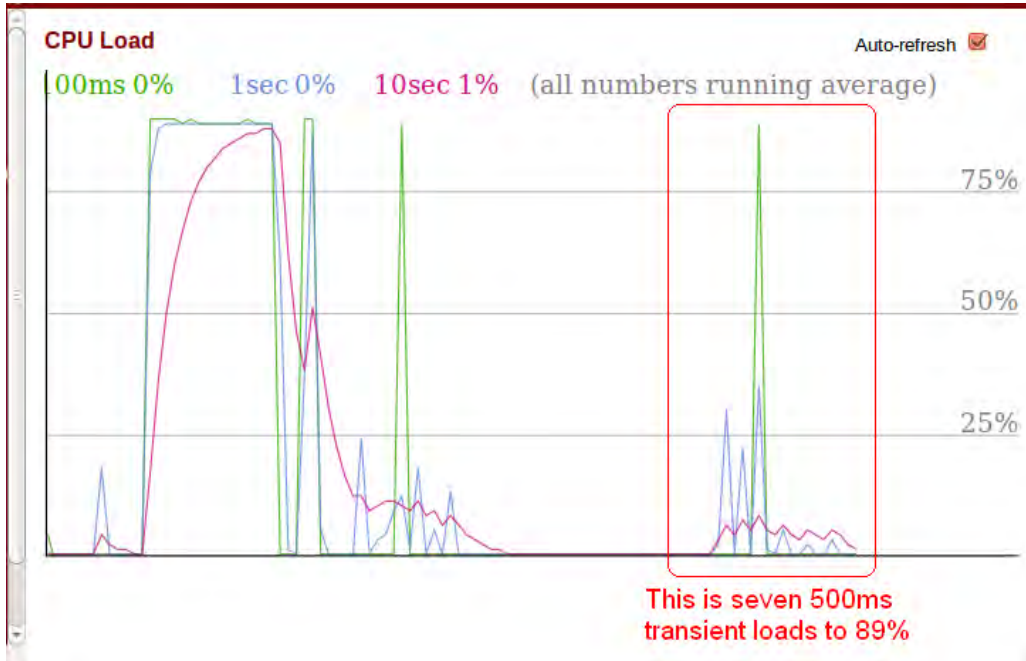
If you let it run for a while, the CPU Load graph will look something like this:

**Buttons**

Auto-refresh: Check this checkbox to enable an automatic page refresh every three seconds.

Example

The screen below shows a workload introduced at 500 ms intervals that creates transient spikes in the graphs to 89% load.



For troubleshooting High CPU utilization conditions, see "[Troubleshooting High CPU Load Conditions](#)" on page 553.

Monitor > System > IP Status

The Monitor > System > IP Status page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbour cache (ARP cache) status.

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

Configuration
 Monitor
 System
 Information
 CPU Load
 IP Status
 Log
 Detailed Log
 Ports
 Link OAM
 DHCP
 Security
 LACP
 Loop Protection
 Spanning Tree
 MVR
 IPMC
 LLDP
 Ethernet Services
 PTP
 MAC Table
 VLANs
 DDMI
 UDLD
 Diagnostics
 Maintenance

Auto-refresh Refresh

IP Interfaces

| Interface | Type | Address | Status |
|-----------|------|-----------------------------|----------------------------------|
| OS:lo | LINK | 00-00-00-00-00-00 | <UP LOOPBACK RUNNING MULTICAST> |
| OS:lo | IPv4 | 127.0.0.1/8 | |
| OS:lo | IPv6 | fe80::1/64 | |
| OS:lo | IPv6 | ::1/128 | |
| VLAN1 | LINK | 00-c0-f2-56-16-d0 | <UP BROADCAST RUNNING MULTICAST> |
| VLAN1 | IPv4 | 192.168.1.11/24 | |
| VLAN1 | IPv6 | fe80::2c0:f2ff:fe56:16d0/64 | |

IP Routes

| Network | Gateway | Status |
|--------------|-----------|-----------|
| 127.0.0.1/32 | 127.0.0.1 | <UP HOST> |
| 224.0.0.0/4 | 127.0.0.1 | <UP> |
| ::1/128 | ::1 | <UP HOST> |

Neighbour cache

| IP Address | Link Address |
|--------------------------|-------------------------|
| 192.168.1.30 | VLAN1:00-04-75-bd-9c-36 |
| fe80::2c0:f2ff:fe56:16d0 | VLAN1:00-c0-f2-56-16-d0 |

IP Interfaces

Interface

The name of the interface (e.g., **OS:lo** or **VLAN1**).

Type

The address type of the entry. This may be **LINK** or **IPv4** or **IPv6**.

Address

The current address of the interface (of the given type).

Status

The status flags of the interface (and/or address). For example: **<UP LOOPBACK RUNNING MULTICAST>** or **<UP BROADCAST RUNNING MULTICAST>**.

IP Routes

Network

The destination IP network or host address of this route (e.g., **192.168.1.0/24** or **224.0.0.0/4** or **::1/128**).

Gateway

The gateway address of this route (e.g., **127.0.0.1** or **VLAN1** or **::1**).

Status

The status flags of the route. For example **<UP HOST>** or **<UP HW_RT>** or **<UP>**.

Neighbour cache

IP Address

The IP address of the entry.

Link Address

The Link (MAC) address for which a binding to the IP address given exists. For example **VLAN1:00-c0-f2-56-19-08**.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh : Check this box to refresh the page automatically every three seconds.

Monitor > System > Log

The **Monitor > System > Log** menu path displays the System Log Information page. The S4224 system log information is provided here. (System Logging is configured from the **Configuration > System > Log** menu path.)

Syslog is a method to collect messages from devices to a server running a syslog **daemon**. Logging to a central syslog server helps in aggregation of logs and alerts which is useful for troubleshooting.

System Log Information

Auto-refresh Refresh Clear << >>

Level: All
Clear Level: All

The total number of entries is 19 for the given level.

Start from ID 1 with 20 entries per page.

| ID | Level | Time | Message |
|----|---------------|---------------------------|---|
| 1 | Informational | 1970-01-01T00:00:09+00:00 | SYS-BOOTING: Switch just made a cool boot. |
| 2 | Notice | 1970-01-01T00:00:09+00:00 | LINK-UPDOWN: Interface Vlan 1, changed state to down. |
| 3 | Informational | 1970-01-01T00:00:09+00:00 | DDMI-MODULE_INSERT_REMOVE: Inserted SFP module on Interface GigabitEthernet 1/23 |
| 4 | Informational | 1970-01-01T00:00:10+00:00 | SyncE selector state change: Free Run |
| 5 | Informational | 1970-01-01T00:00:15+00:00 | DDMI-TEMPERATURE_CHANGED: DoM temperature changed to REGULAR on Interface GigabitEthernet 1/... |
| 6 | Informational | 1970-01-01T00:00:15+00:00 | DDMI-VOLTAGE_CHANGED: DoM voltage changed to REGULAR on Interface GigabitEthernet 1/23 |
| 7 | Informational | 1970-01-01T00:00:15+00:00 | DDMI-BIAS_CHANGED: DoM Bias changed to REGULAR on Interface GigabitEthernet 1/23 |
| 8 | Informational | 1970-01-01T00:00:15+00:00 | DDMI-BIAS_CHANGED: DoM Tx Power changed to REGULAR on |
| 9 | Informational | 1970-01-01T00:00:15+00:00 | DDMI-BIAS_CHANGED: DoM Rx Power changed to LO ALARM on Interface GigabitEthernet 1/23 |
| 10 | Informational | 1970-01-01T00:00:15+00:00 | DDMI-MODULE_INSERT_REMOVE: Inserted SFP module on Interface 10GigabitEthernet 1/4 |
| 11 | Notice | 1970-01-01T00:00:17+00:00 | LINK-UPDOWN: Interface ManagementPort 1/1, changed state to up. |
| 12 | Notice | 1970-01-01T00:00:18+00:00 | LINK-UPDOWN: Interface Vlan 1, changed state to up. |
| 13 | Informational | 1970-01-01T00:00:19+00:00 | Power supply 1 present |
| 14 | Informational | 1970-01-01T00:00:19+00:00 | Power supply 2 present |
| 15 | Notice | 1970-01-01T00:00:19+00:00 | LINK-UPDOWN: Interface Vlan 1, changed state to up. |

For detailed syslog information, click a linked ID number in one of the lines.

The S4224 system log information is explained below.

ID

The ID of the system log entry. Each ID is hot linked to its details page.

Level

The level of the system log entry. The following level types are supported:

Error: Error level of the system log (Severity 3). Non-urgent failures - these should be relayed to developers or admins. Each item must be resolved within a given time.

Warning: Warning level of the system log (Severity 4). Warning messages - not an error, but indication that an error will occur if action is not taken (e.g. *file system 85% full*). Each item must be resolved within a given time.

Informational: Information level of the system log (Severity 6). Normal operational messages - used for reporting, measuring throughput, etc. - require no action.

Notice: Notice level (e.g., *LINK-UPDOWN: Interface Vlan 1, changed state to down.*). Severity 5: Normal but significant condition.

All: All four levels of information are logged (Info, Warning, Error and Notice).

Time

The time of the system log entry. The format is *yyyy-mm-ddThh:mm:ss+<offset>*. For example: *"1970-01-03T18:15:35+00:00"*.

Message

The message of the system log entry. If the selected level has no syslog info to report, the message “*No system log entries*” displays. See “[System Log Messages](#)” on page 594 for more information.

Buttons

Auto-refresh: Check this checkbox to automatically refresh the page every three seconds. .

Refresh: Updates the system log entries, starting from the current entry ID. **Note:** Repeated **Refresh** button action causes configuration display changes with each refresh action (e.g., displays "level" = warning, "clear level"= all, press F5/Refresh; "clear level"= "error"; press F5; the configuration goes back to "clear level"= all).

Clear: Flushes all system log entries.

|<<: First page; updates the system log entries, starting from the first available entry ID.

<<: Previous page; updates the system log entries, ending at the last entry currently displayed.

>>: Next page; updates the system log entries, starting from the last entry currently displayed.

>>|: Last page; updates the system log entries, ending at the last available entry ID.

See “[System Log Messages](#)” on page 594 for more information.

Detailed System Log Information

You can access the syslog details either by clicking on an **ID** column number in the System Log Information table, or via the **Monitor > System > Detailed Log** menu path.

Use the browser's Back button to return to the **Monitor > System > Log** page.

System Log Message Summary

The System Log information is summarized below in terms of syslog level, message, and description.

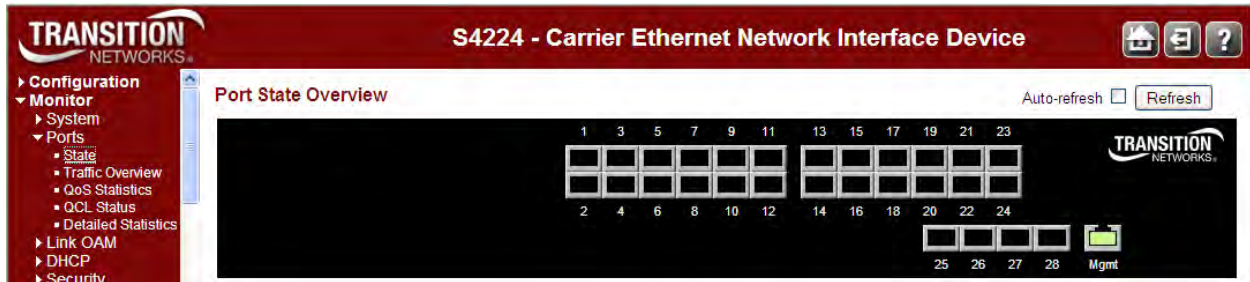
| Level | Sample Message | Description |
|----------------|---|--|
| Info | <i>Switch just made a cool boot.</i> | The S4224 was restarted. See " Maintenance > Restart Device ". |
| | <i>Link up on port x</i> | The most recent link status on the port x is 'link up'. Port Link is up - no action needed. |
| | <i>Link down on port x</i> | The most recent link status on the port x is 'link down'. See Configuration > Ports > Port Configuration . |
| | <i>Using primary power source.</i> | Normal power on operation. |
| | <i>Frame of 243 bytes received on port 1MAC</i> | Normal frame size information. |
| | <i>Port 1 shut down</i> | Normal port shutdown information. |
| | <i>Authentication for 'admin' successful via 'console'</i> | Normal authentication succes via Console device |
| Warning | <i>E api/cil 17:42:26 29/26_action_check#6036:</i> | ACL policer and EVC policer can not both be enabled. Disable one or the other. |
| Error | <i>E api/cil 17:42:45 29/26_acl_policer_free#6069:</i> | Error: policer 0 already free. The EVC policer or ... |
| | <i>VLAN Port Configuration Ingress Filter Conflict - MSTP</i> | Verify the Ingress Policers, Port Policing, or Queue Policing configuration. See the Configuration > Security > Network > ACL or QoS menu path. |
| | <i>VLAN Port Configuration Ingress Filter Conflict - ERPS</i> | Verify the ERPS config at the Configuration > ERPS . |
| Notice | <i>LINK-UPDOWN: Interface Vlan 1, changed state to up.</i> | Link state changes from down to up. |

See "[System Log Messages](#)" on page 594 for System Log message descriptions.

Monitor > Ports > State

From the **Monitor > Ports > State** menu path you can view the Port State Overview table.

This page provides an overview of the current S4224 port states.



The S4224 port states are shown and explained below.

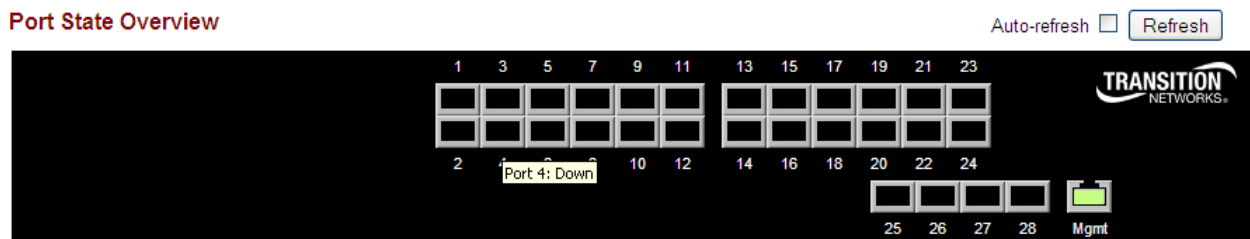
| Port | State | | |
|------------|----------|------|------|
| | Disabled | Down | Link |
| RJ45 ports | | | |
| SFP ports | | | |
| X2 ports | | | |

Buttons

Auto-refresh: Check this box to refresh the page automatically every three seconds.

Refresh: Click to refresh the page; any changes made locally will be undone.

Hover the cursor over a port for the speed of that port (e.g., *Port 1: Up*, or *Port 2: Down*, or *Port 5: 100fdx*). For example:



Detailed Port Statistics

Left mouse click on a port to display that port's 'Detailed Port Statistics' page. (You can also reach this page from the **Monitor > Ports > Detailed Statistics** menu path.) See "[Detailed Port Statistics](#)" on page 391 for more information on the 'Detailed Port Statistics' parameters. A sample 'Detailed Port Statistics' page is shown below (for Port 4).

S4224 - Carrier Ethernet Network Interface Device

Detailed Port Statistics Port 4 Port 4 Auto-refresh

| Receive Total | | Transmit Total | |
|------------------------|---|-------------------------|---|
| Rx Packets | 0 | Tx Packets | 0 |
| Rx Octets | 0 | Tx Octets | 0 |
| Rx Unicast | 0 | Tx Unicast | 0 |
| Rx Multicast | 0 | Tx Multicast | 0 |
| Rx Broadcast | 0 | Tx Broadcast | 0 |
| Rx Pause | 0 | Tx Pause | 0 |
| Receive Size Counters | | Transmit Size Counters | |
| Rx 64 Bytes | 0 | Tx 64 Bytes | 0 |
| Rx 65-127 Bytes | 0 | Tx 65-127 Bytes | 0 |
| Rx 128-255 Bytes | 0 | Tx 128-255 Bytes | 0 |
| Rx 256-511 Bytes | 0 | Tx 256-511 Bytes | 0 |
| Rx 512-1023 Bytes | 0 | Tx 512-1023 Bytes | 0 |
| Rx 1024-1526 Bytes | 0 | Tx 1024-1526 Bytes | 0 |
| Rx 1527- Bytes | 0 | Tx 1527- Bytes | 0 |
| Receive Queue Counters | | Transmit Queue Counters | |
| Rx Q0 | 0 | Tx Q0 | 0 |
| Rx Q1 | 0 | Tx Q1 | 0 |
| Rx Q2 | 0 | Tx Q2 | 0 |
| Rx Q3 | 0 | Tx Q3 | 0 |
| Rx Q4 | 0 | Tx Q4 | 0 |
| Rx Q5 | 0 | Tx Q5 | 0 |
| Rx Q6 | 0 | Tx Q6 | 0 |
| Rx Q7 | 0 | Tx Q7 | 0 |
| Receive Error Counters | | Transmit Error Counters | |
| Rx Drops | 0 | Tx Drops | 0 |
| Rx CRC/Alignment | 0 | Tx Late/Exc. Coll. | 0 |
| Rx Undersize | 0 | | |
| Rx Oversize | 0 | | |
| Rx Fragments | 0 | | |
| Rx Jabber | 0 | | |
| Rx Filtered | 0 | | |

Buttons

Port 1 The port select box determines which port is affected by clicking the buttons.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

Auto-refresh: Check this box to automatically refresh the page every three seconds.

Monitor > Ports > Traffic Overview

From the **Monitor > Ports > Traffic Overview** menu path you can view the Port Statistics Overview table. This page provides an overview of general traffic statistics for all S4224 ports.

| Port | Packets | | Bytes | | Errors | | Drops | | Filtered |
|------|----------|-------------|----------|-------------|----------|-------------|----------|-------------|----------|
| | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received |
| 1 | 0 | 38 | 0 | 12182 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 13 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 14 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 17 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 18 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 19 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 20 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 21 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 22 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 23 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 24 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 25 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 26 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 27 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 28 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 29 | 6374 | 4977 | 1588055 | 1311613 | 5 | 0 | 5 | 0 | 5 |

The displayed counters are explained below.

Port

The logical port for the settings contained in the same row. Provides a link to the Detailed Port Statistics page for each port.

Packets

The number of received and transmitted packets per port.

Bytes

The number of received and transmitted bytes per port.

Errors

The number of frames received in error and the number of incomplete transmissions per port.

Drops

The number of frames discarded due to ingress or egress congestion.

Filtered

The number of received frames filtered by the forwarding process.

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

Auto-refresh: Check this checkbox to automatically refresh the page every three seconds. .

Left mouse click on a port to display that port's 'Detailed Port Statistics' page. (You can also reach this page from the **Monitor > Ports > Detailed Statistics** menu path.) See '[Detailed Port Statistics](#)' on page 391 for more information on the 'Detailed Port Statistics' parameters.

Example

The screen below shows Port Statistics reporting Port 3 dropping traffic:

Port Statistics Overview Auto-refresh Refresh Clear

| Port | Packets | | Bytes | | Errors | | Drops | | Filtered |
|------|----------|-------------|----------|-------------|----------|-------------|----------|-------------|----------|
| | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 687757 | 146 | 44016448 | 17931 | 0 | 0 | 0 | 0 | 687757 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 399 | 694 | 34123 | 61223 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Monitor > Ports > QoS Statistics

From the **Monitor > Ports > QoS Statistics** menu path you can view the Queuing Counters page. This page provides statistics for the various queues for all S4224 ports.

The S4224 supports eight transmission queues per port based on user priority of each frame. This gives you the option to change the output queue mapping based on priority. Statistics for each output queue on each port are available. The option to restrict a port to a specific number of MAC entries to be learned is provided to allow the provider to restrict number of devices that can be serviced by this port.

S4224 - Carrier Ethernet Network Interface Device

Queuing Counters

Auto-refresh Refresh Clear

| Port | Q0 | | Q1 | | Q2 | | Q3 | | Q4 | | Q5 | | Q6 | | Q7 | |
|------|------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------|
| | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx |
| 1 | 0 | 38 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 13 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 14 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 17 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 18 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 19 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 20 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 21 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 22 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 23 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 24 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 25 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 26 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 27 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 28 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 29 | 6407 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 5003 |

The displayed QoS Statistics counters are explained below.

Port

The logical port for the settings contained in the same row. Click on an individual port number in the 'Port' column to display the Detailed Port Statistics for that port.

Qn

There are eight QoS queues per port (Q0-Q7). Q0 is the lowest priority queue.

Rx

The number of received packets per queue.

Tx

The number of transmitted packets per queue.

Buttons

Auto-refresh: Click to refresh the page immediately.

Refresh: Clears the counters for all ports.

Auto-refresh: Check this checkbox to automatic allyrefresh this page every three seconds.

See '[Detailed Port Statistics](#)' on page 391 for more information on the 'Detailed Port Statistics' parameters.

Monitor > Ports > QCL Status

From the **Monitor > Ports > QCL Status** menu path you can view the QoS Control List Status table. This page shows the QCL status by different QCL users.

| User | QCE | Port | Frame Type | Action | | | | | | Conflict |
|--------|-----|-------|------------|--------|---------|---------|---------|---------|--------|----------|
| | | | | CoS | DPL | DSCP | PCP | DEI | Policy | |
| Static | 1 | 2,5,6 | Any | 0 | Default | Default | Default | Default | 1 | No |

Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The S4224 supports up to **256** QCEs.

The displayed **QoS Control List Status** table parameters are explained below.

QCL Status to Display

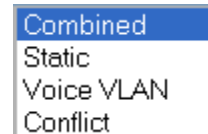
From the dropdown list, select the QCL status to be displayed:

Combined: Displays the 'Static' and 'Conflict' QCL status.

static: Displays just the 'Static' QCL status.

Voice VLAN: Displays just the Voice VLAN status.

Conflict: Displays just the 'Conflict' QCL status.



User

Indicates the QCL user type selected for display (e.g., Combined, Static, or Conflict).

QCE

Indicates the index of the QCE on this line of the table.

Port

Indicates the list of ports configured with the QCE.

Frame Type

Indicates the type of frame to look for incoming frames. The QCE frame types are defined at the **Configuration > QoS > QoS Control List** menu path. Possible frame types are:

Any: Match any frame type.

Ethernet: Match EtherType frames (Ether Type 0x600-0xFFFF).

LLC: Match only LLC frames.

SNAP: Match only SNAP frames. (The SubNetwork Access Protocol (SNAP) mechanism for multiplexing, on networks using IEEE 802.2 LLC.)

IPv4: Match only IPV4 frames.

IPv6: Match only IPV6 frames.

Action

Indicates the classification action taken on ingress frames if parameters configured are matched with the frame's content. The possible actions are:

CoS: Classify Class of Service.

DPL: Classify Drop Precedence Level.

DSCP: Classify DSCP value.

Conflict

Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications, it may happen that resources required to add a QCE may not be available. In that case it shows conflict status as 'Yes', otherwise it is always 'No'. Note that conflict can be resolved by releasing the hardware resources required to add a QCL entry on pressing the '**Resolve Conflict**' button.

Buttons

: Select the QCL status from this drop down list (**Combined**, **Static**, or **Conflict**).

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Resolve Conflict: Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.

Refresh: Click to refresh the page; any changes made locally will be undone.

Monitor > Ports > Detailed Statistics

The **Monitor > Ports > Detailed Statistics** menu path displays the Detailed Port Statistics page for a Port. This page provides detailed traffic statistics for a specific S4224 port. Use the port select box

(Port 1) , to select which port details to display.

The S4224 provides MAC bridging functionality per IEEE 802.1D. The S4224 can operate in a VLAN unaware mode where it is an open bridge. The S4224 can forward unicast, multicast, or broadcasts frames. RMON Counters based on frame type / frame size are maintained and reported. All error counters at the MAC layer are reported per ether-like MIB (RFC 2665) and/or IF-MIB (RFC 2863).

S4224 - Carrier Ethernet Network Interface Device

Detailed Port Statistics Port 1 Port 1 Auto-refresh Refresh Clear

| Receive Total | | Transmit Total | |
|------------------------|---|-------------------------|-------|
| Rx Packets | 0 | Tx Packets | 38 |
| Rx Octets | 0 | Tx Octets | 12182 |
| Rx Unicast | 0 | Tx Unicast | 38 |
| Rx Multicast | 0 | Tx Multicast | 0 |
| Rx Broadcast | 0 | Tx Broadcast | 0 |
| Rx Pause | 0 | Tx Pause | 0 |
| Receive Size Counters | | Transmit Size Counters | |
| Rx 64 Bytes | 0 | Tx 64 Bytes | 18 |
| Rx 65-127 Bytes | 0 | Tx 65-127 Bytes | 0 |
| Rx 128-255 Bytes | 0 | Tx 128-255 Bytes | 0 |
| Rx 256-511 Bytes | 0 | Tx 256-511 Bytes | 0 |
| Rx 512-1023 Bytes | 0 | Tx 512-1023 Bytes | 20 |
| Rx 1024-1526 Bytes | 0 | Tx 1024-1526 Bytes | 0 |
| Rx 1527- Bytes | 0 | Tx 1527- Bytes | 0 |
| Receive Queue Counters | | Transmit Queue Counters | |
| Rx Q0 | 0 | Tx Q0 | 38 |
| Rx Q1 | 0 | Tx Q1 | 0 |
| Rx Q2 | 0 | Tx Q2 | 0 |
| Rx Q3 | 0 | Tx Q3 | 0 |
| Rx Q4 | 0 | Tx Q4 | 0 |
| Rx Q5 | 0 | Tx Q5 | 0 |
| Rx Q6 | 0 | Tx Q6 | 0 |
| Rx Q7 | 0 | Tx Q7 | 0 |
| Receive Error Counters | | Transmit Error Counters | |
| Rx Drops | 0 | Tx Drops | 0 |
| Rx CRC/Alignment | 0 | Tx Late/Exc. Coll. | 0 |
| Rx Undersize | 0 | | |
| Rx Oversize | 0 | | |
| Rx Fragments | 0 | | |
| Rx Jabber | 0 | | |
| Rx Filtered | 0 | | |

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Receive Total and Transmit Total

Rx and Tx Packets

The number of received and transmitted (good and bad) packets.

Rx and Tx Octets

The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

Rx and Tx Unicast

The number of received and transmitted (good and bad) unicast packets.

Rx and Tx Multicast

The number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast

The number of received and transmitted (good and bad) broadcast packets.

Rx and Tx Pause

A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters

The number of received and transmitted packets per input and output queue.

Receive Error Counters

Rx Drops

The number of frames dropped due to lack of receive buffers or egress congestion.

Rx CRC/Alignment

The number of frames received with CRC or alignment errors.

Rx Undersize

The number of short frames received with valid CRC. 'Short frames' are frames that are smaller than 64 bytes.

Rx Oversize

The number of long frames received with valid CRC. 'Long frames' are frames that are longer than the configured maximum frame length for this port.

Rx Fragments

The number of short frames received with invalid CRC. 'Short frames' are frames that are smaller than 64 bytes.

Rx Jabber

The number of long frames received with invalid CRC. 'Long frames' are frames that are longer than the configured maximum frame length for this port.

Rx Filtered

The number of received frames filtered by the forwarding process.

Transmit Error Counters

Tx Drops

The number of frames dropped due to output buffer congestion.

Tx Late/Exc. Coll.

The number of frames dropped due to excessive or late collisions.

Buttons



: The port select box determines which port is affected.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

Auto-refresh: Check this box to automatically refresh the page every three seconds.

Monitor > Link OAM > Statistics

The **Monitor > Link OAM > Statistics** menu path displays the Detailed Link OAM Statistics for a Port.

This page provides detailed LOAM traffic statistics for a specific S4224 port. Use the port select box to select which S4224 port details to display.

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

Configuration
 Monitor
 System
 Ports
 Link OAM
 Statistics
 Port Status
 Event Status
 DHCP
 Security
 LACP
 Loop Protection
 Spanning Tree
 MVR
 IPMC
 LLDP

Detailed Link OAM Statistics for Port 1

Port 1 Auto-refresh Refresh Clear

| Receive Total | | Transmit Total | |
|---------------------------------------|---|---------------------------------------|---|
| Rx OAM Information PDU's | 0 | Tx OAM Information PDU's | 0 |
| Rx Unique Error Event Notification | 0 | Tx Unique Error Event Notification | 0 |
| Rx Duplicate Error Event Notification | 0 | Tx Duplicate Error Event Notification | 0 |
| Rx Loopback Control | 0 | Tx Loopback Control | 0 |
| Rx Variable Request | 0 | Tx Variable Request | 0 |
| Rx Variable Response | 0 | Tx Variable Response | 0 |
| Rx Org Specific PDU's | 0 | Tx Org Specific PDU's | 0 |
| Rx Unsupported Codes | 0 | Tx Unsupported Codes | 0 |
| Rx Link Fault PDU's | 0 | Tx Link Fault PDU's | 0 |
| Rx Dying Gasp | 0 | Tx Dying Gasp | 0 |
| Rx Critical Event PDU's | 0 | Tx Critical Event PDU's | 0 |

The displayed counters represent the total number of OAM frames received and transmitted for the selected port. Discontinuities of these counters can occur at re-initialization of the management system.

Receive Total and Transmit Total

Rx and Tx OAM Information PDU's

The number of received and transmitted OAM Information PDU's. Discontinuities of this counter can occur at re-initialization of the management system.

Rx and Tx Unique Error Event Notification

A count of the number of unique Event OAMPDUs received and transmitted on this interface. Event Notifications may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. Duplicate Event Notification transmissions are counted by Duplicate Event Notification counters for Tx and Rx respectively. A unique Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is distinct from the previously transmitted Event Notification OAMPDU Sequence Number.

Rx and Tx Duplicate Error Event Notification

A count of the number of duplicate Event OAMPDUs received and transmitted on this interface. Event Notification OAMPDUs may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. A duplicate Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is identical to the previously transmitted Event Notification OAMPDU Sequence Number.

Rx and Tx Loopback Control

A count of the number of Loopback Control OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Request

A count of the number of Variable Request OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Response

A count of the number of Variable Response OAMPDUs received and transmitted on this interface.

Rx and Tx Org Specific PDU's

A count of the number of Organization Specific OAMPDUs transmitted on this interface.

Rx and Tx Unsupported Codes

A count of the number of OAMPDUs transmitted on this interface with an unsupported op-code.

Rx and Tx Link fault PDU's

A count of the number of Link fault PDU's received and transmitted on this interface.

Rx and Tx Dying Gasp


A count of the number of Dying Gasp events received and transmitted on this interface (Last Gasp). The S4224 is equipped with the last gasp circuit for triggering a notification in the event of a power failure.

This can be useful for sending a notification. The uplink ports have highest priority to send the notifications of last gasp. The last gasp can be in the form of IEEE802.3 2008 Clause 57 Dying gasp event and/or an SNMP trap to NMS system. The management interface provides an option to choose the preferred mode of notification (either a SNMP trap and/or an IEEE 802.3 2008 clause 57 event).

Rx and Tx Critical Event PDU's

A count of the number of Critical event PDU's received and transmitted on this interface.

Buttons

: The port select box defines which port is affected by clicking the buttons.

Auto-refresh: Check this checkbox to enable automatic refreshes of the page at 3 second intervals.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

Monitor > Link OAM > Port Status

The **Monitor > Link OAM > Port Status** menu path displays the Detailed Link OAM Status for an S4224 port. This page provides Link OAM configuration and operational status.

S4224 - Carrier Ethernet Network Interface Device

Port 28 Auto-refresh Refresh

Detailed Link OAM Status for Port 28

| | |
|------------------|---------------|
| PDU Permission | Info exchange |
| Discovery State | Active state |
| Peer MAC Address | ----- |

| Local | | Peer | |
|--------------------------------------|------------|--------------------------------------|-------|
| Mode | Active | Mode | ----- |
| Unidirectional Operation Support | Disabled | Unidirectional Operation Support | ----- |
| Remote Loopback Support | Disabled | Remote Loopback Support | ----- |
| Link Monitoring Support | Enabled | Link Monitoring Support | ----- |
| MIB Retrieval Support | Disabled | MIB Retrieval Support | ----- |
| MTU Size | 1500 | MTU Size | ----- |
| Multiplexer State | Forwarding | Multiplexer State | ----- |
| Parser State | Forwarding | Parser State | ----- |
| Organizational Unique Identification | 00-c0-f2 | Organizational Unique Identification | ----- |
| PDU Revision | 0 | PDU Revision | ----- |

The displayed fields show the active configuration status for the selected port.

PDU Permission

This field is available only for the Local DTE. It displays the current permission rules set for the local DTE. Possible values are "Link fault", "Receive only", "Info exchange", or "ANY".

Discovery State

Displays the current state of the discovery process. Possible states are Fault state, Active state, Passive state, SEND_LOCAL_REMOTE_STATE, SEND_LOCAL_REMOTE_OK_STATE, SEND_ANY_STATE.

Peer MAC Address

Displays the MAC address of the peer if known; displays "-----" if not known.

Local and Peer

Mode

The Mode in which the Link OAM is operating, Active or Passive.

Unidirectional Operation Support

This feature is not user-configurable. The status of this configuration is retrieved from the PHY.

Remote Loopback Support

If status is enabled, DTE is capable of OAM remote loopback mode.

Link Monitoring Support

If status is enabled, DTE supports interpreting Link Events.

MIB Retrieval Support

If status is enabled DTE supports sending Variable Response OAMPDUs.

MTU Size

It represents the largest OAMPDU, in octets, supported by the DTE. This value is compared to the remotes Maximum PDU Size and the smaller of the two is used.

Multiplexer State

When in 'Forwarding' state, the S4224 is forwarding non-OAMPDUs to the lower sublayer. In the case of discarding, the S4224 discards all the non-OAMPDUs.

Parser State

When in 'Forwarding' state, the S4224 is forwarding non-OAMPDUs to a higher sublayer.
When in 'Loopback' state, the S4224 is looping back non-OAMPDUs to the lower sublayer.
When in 'Discarding' state, the S4224 is discarding non-OAMPDUs.

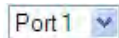
Organizational Unique Identification

This is the 24-bit Organizationally Unique Identifier (OUI) of the vendor (e.g., 00-C0-F2).

PDU Revision

Indicates the current revision of the Information TLV. The value of this field starts at zero and is incremented each time something in the Information TLV changes. Upon reception of an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed (an Information TLV that is identical to the previous Information TLV doesn't need to be parsed as nothing in it has changed).

Buttons



: Use the port select box to define which port is affected by clicking the buttons.

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this checkbox to automatically refresh the page every three seconds. .

Monitor > Link OAM > Event Status

The **Monitor > Link OAM > Event Status** menu path displays detailed Link OAM (LOAM) Link Status for an S4224 port.

This page lets you view the current Link OAM Link Event configurations.

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

Detailed Link OAM Link Status for Port 1

Port 1 Auto-refresh Refresh

| Local Frame Error Status | | Remote Frame Error Status | |
|-------------------------------------|---|-------------------------------------|---|
| Sequence Number | 0 | | |
| Frame Error Event Timestamp | 0 | Frame Error Event Timestamp | 0 |
| Frame error event window | 0 | Frame error event window | 0 |
| Frame error event threshold | 0 | Frame error event threshold | 0 |
| Frame errors | 0 | Frame errors | 0 |
| Total frame errors | 0 | Total frame errors | 0 |
| Total frame error events | 0 | Total frame error events | 0 |
| Local Frame Period Status | | Remote Frame Period Status | |
| Frame Period Error Event Timestamp | 0 | Frame Period Error Event Timestamp | 0 |
| Frame Period Error Event Window | 0 | Frame Period Error Event Window | 0 |
| Frame Period Error Event Threshold | 0 | Frame Period Error Event Threshold | 0 |
| Frame Period Errors | 0 | Frame Period Errors | 0 |
| Total frame period errors | 0 | Total frame period errors | 0 |
| Total frame period error events | 0 | Total frame period error events | 0 |
| Local Symbol Period Status | | Remote Symbol Period Status | |
| Symbol Period Error Event Timestamp | 0 | Symbol Period Error Event Timestamp | 0 |
| Symbol Period Error Event Window | 0 | Symbol Period Error Event Window | 0 |
| Symbol Period Error Event Threshold | 0 | Symbol Period Error Event Threshold | 0 |
| Symbol Period Errors | 0 | Symbol Period Errors | 0 |
| Symbol frame period errors | 0 | Symbol frame period errors | 0 |
| Symbol frame period error events | 0 | Symbol frame period error events | 0 |
| Local Event Seconds Summary Status | | Remote Event Seconds Summary Status | |
| Event Seconds Summary Time Stamp | 0 | Event Seconds Summary Time Stamp | 0 |
| Event Seconds Summary Window | 0 | Event Seconds Summary Window | 0 |
| Event Seconds Summary Threshold | 0 | Event Seconds Summary Threshold | 0 |
| Event Seconds Summary Events | 0 | Event Seconds Summary Events | 0 |
| Event Seconds Summary Error Total | 0 | Event Seconds Summary Error Total | 0 |
| Event Seconds Summary Event Total | 0 | Event Seconds Summary Event Total | 0 |

The left pane displays the Event status for the Local OAM unit while the right pane displays the status for the Peer for the respective port.

Port dropdown

Port 1 Use to select the S4224 port number.

Frame Error Event Timestamp

This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Frame error event window

This two-octet field indicates the duration of the period in terms of 100 ms intervals. The default value is one second. The lower bound is one second. The upper bound is one minute.

Frame error event threshold

This four-octet field indicates the number of detected errored frames in the period is required to be equal to or greater than in order for the event to be generated. The default value is one frame error. The lower bound is zero frame errors. The upper bound is unspecified.

Frame errors

This four-octet field indicates the number of detected errored frames in the period.

Total frame errors

This eight-octet field indicates the sum of errored frames that have been detected since the OAM sublayer was reset.

Total frame error events

This four-octet field indicates the number of Errored Frame Event TLVs that have been generated since the OAM sublayer was reset.

Frame Period Error Event Timestamp

This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Frame Period Error Event Window

This four-octet field indicates the duration of period in terms of frames.

Frame Period Error Event Threshold

This four-octet field indicates the number of errored frames in the period is required to be equal to or greater than in order for the event to be generated.

Frame Period Errors

This four-octet field indicates the number of frame errors in the period.

Total frame period errors

This eight-octet field indicates the sum of frame errors that have been detected since the OAM sublayer was reset.

Total frame period error events

This four-octet field indicates the number of Errored Frame Period Event TLVs that have been generated since the OAM sublayer was reset.

Symbol Period Error Event Timestamp

This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Symbol Period Error Event Window

This eight-octet field indicates the number of symbols in the period.

Symbol Period Error Event Threshold

This eight-octet field indicates the number of errored symbols in the period is required to be equal to or greater than in order for the event to be generated.

Symbol Period Errors

This eight-octet field indicates the number of symbol errors in the period.

Symbol frame period errors

This eight-octet field indicates the sum of symbol errors since the OAM sublayer was reset.

Symbol frame period error events

This four-octet field indicates the number of Errored Symbol Period Event TLVs that have been generated since the OAM sublayer was reset.

Event Seconds Summary Time Stamp

This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

Event Seconds Summary Window

This two-octet field indicates the duration of the period in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

Event Seconds Summary Threshold

This two-octet field indicates the number of errored frame seconds in the period is required to be equal to or greater than in order for the event to be generated, encoded as a 16-bit unsigned integer.

Event Seconds Summary Events

This two-octet field indicates the number of errored frame seconds in the period, encoded as a 16-bit unsigned integer.

Event Seconds Summary Error Total

This four-octet field indicates the sum of errored frame seconds that have been detected since the OAM sublayer was reset.

Event Seconds Summary Event Total

This four-octet field indicates the number of Errored Frame Seconds Summary Event TLVs that have been generated since the OAM sublayer was reset, encoded as a 32-bit unsigned integer.

Buttons

: Use the port select box to define which port is affected by clicking the buttons.

Refresh: Click to refresh the page.

Clear: Click to clear the data.

Monitor > DHCP > Server

A DHCP server can provide optional configuration parameters to the client. IETF [RFC 2132](#) describes the available DHCP options.

Monitor > DHCP > Server > Statistics

The **Monitor > DHCP > Server > Statistics** page displays the database counters and the number of DHCP messages sent and received by DHCP server.

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

Configuration > Monitor > DHCP > Server > Statistics

Auto-refresh Refresh Clear

DHCP Server Statistics

Database Counters

| Pool | Excluded IP Address | Declined IP Address |
|------|---------------------|---------------------|
| 1 | 1 | 0 |

Binding Counters

| Automatic Binding | Manual Binding | Expired Binding |
|-------------------|----------------|-----------------|
| 0 | 0 | 0 |

DHCP Message Received Counters

| DISCOVER | REQUEST | DECLINE | RELEASE | INFORM |
|----------|---------|---------|---------|--------|
| 0 | 0 | 0 | 0 | 0 |

DHCP Message Sent Counters

| OFFER | ACK | NAK |
|-------|-----|-----|
| 0 | 0 | 0 |

Database Counters

Displays the counters of the various databases.

Pool

Number of the pool.

Excluded IP Address

Number of excluded IP address ranges.

Declined IP Address

Number of declined IP addresses.

Binding Counters

Displays the counters of the various databases.

Automatic Binding

Number of bindings with network-type pools.

Manual Binding

Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type.

Expired Binding

Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.

DHCP Message Received Counters

Display counters of DHCP messages received by DHCP server.

DISCOVER

Number of DHCP DISCOVER messages received.

REQUEST

Number of DHCP REQUEST messages received.

DECLINE

Number of DHCP DECLINE messages received.

RELEASE

Number of DHCP RELEASE messages received.

INFORM

Number of DHCP INFORM messages received.

DHCP Message Sent Counters

Display counters of DHCP messages sent by DHCP server.

OFFER

Number of DHCP OFFER messages sent.

ACK

Number of DHCP ACK messages sent.

NAK

Number of DHCP NAK messages sent.

Buttons

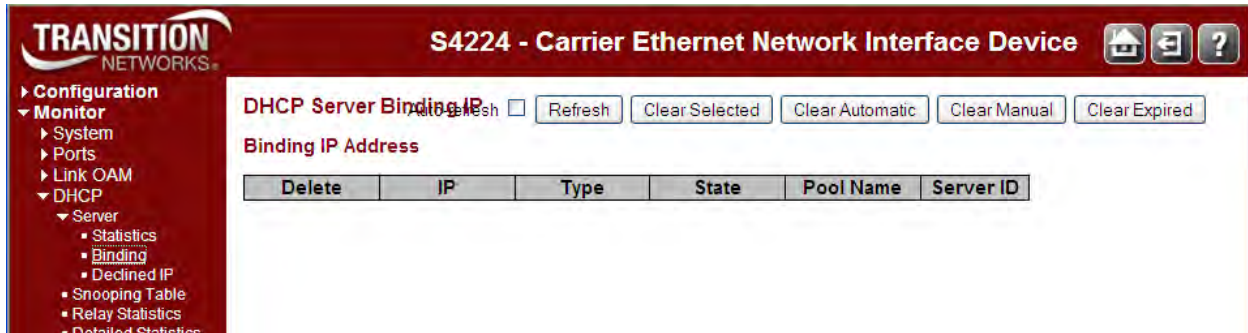
Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Click to clear DHCP Message Received Counters and DHCP Message Sent Counters.

Monitor > DHCP > Server > Binding

The **Monitor > DHCP > Server > Binding** page displays bindings generated for DHCP clients.



The parameters are described below.

Binding IP Address

Displays all bindings.

IP

IP address allocated to DHCP client.

Type

Type of binding. Possible types are *Automatic*, *Manual*, and *Expired*.

State

State of binding. Possible states are *Committed*, *Allocated*, and *Expired*.

Pool Name

The pool that generates the binding.

Server ID

Server IP address to service the binding.

Buttons

Auto-refresh : Check this box to refresh the page automatically every three seconds.

Refresh: Click to refresh the page immediately.

Clear Selected: Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is Expired, then it is freed.

Clear Automatic: Click to clear all Automatic bindings and change them to Expired bindings.

Clear Manual: Click to clear all Manual bindings and change them to Expired bindings.

Clear Expired: Click to clear all Expired bindings and free them.

Monitor > DHCP > Server > Declined IP

The **Monitor > DHCP > Server > Declined IP** page displays declined IP addresses.



Declined IP Addresses

Displays IP addresses declined by DHCP clients, if any exist.

Declined IP

List of IP addresses declined. Typically, no user action is needed. The DHCP service responds to the DHCPDECLINE message with a DHCPNAK message. This response forces the client to release its current IP address and return to its initializing state. The client then attempts to lease a new IP address from the server.

Buttons

Auto-refresh : Check this box to refresh the page automatically every three seconds.

Refresh: Click to refresh the page immediately.

Monitor > DHCP > Snooping Table

The **Monitor > DHCP > Snooping Table** displays the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

Dynamic DHCP Snooping Table

Auto-refresh Refresh << >>

Start from MAC address 00-00-00-00-00-00 , VLAN 0 with 20 entries per page.

| MAC Address | VLAN ID | Source Port | IP Address | IP Subnet Mask | DHCP Server |
|-----------------|---------|-------------|------------|----------------|-------------|
| No more entries | | | | | |

Each page shows up to 99 entries from the Dynamic DHCP snooping table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic DHCP Snooping Table.

The "MAC address" and "VLAN" input fields let you select the starting point in the Dynamic DHCP snooping Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next Dynamic DHCP snooping Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

DHCP Snooping Table Columns

MAC Address

User MAC address of the entry.

VLAN ID

VLAN-ID in which the DHCP traffic is permitted.

Source Port

Switch Port Number for which the entries are displayed.

IP Address

User IP address of the entry.

IP Subnet Mask

User IP subnet mask of the entry.

DHCP Server Address

DHCP Server address of the entry.

Buttons

Auto-refresh : Check this box to refresh the page automatically every three seconds.

Refresh: Refreshes the displayed table starting from the input fields.

Clear: Flushes all dynamic entries.

|<<: Updates the table starting from the first entry in the Dynamic DHCP Snooping Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

Monitor > DHCP > Relay Statistics

This page provides statistics for DHCP Relay. DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Relay Statistics Auto-refresh Refresh Clear

Server Statistics

| Transmit to Server | Transmit Error | Receive from Server | Receive Missing Agent Option | Receive Missing Circuit ID | Receive Missing Remote ID | Receive Bad Circuit ID | Receive Bad Remote ID |
|--------------------|----------------|---------------------|------------------------------|----------------------------|---------------------------|------------------------|-----------------------|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Client Statistics

| Transmit to Client | Transmit Error | Receive from Client | Receive Agent Option | Replace Agent Option | Keep Agent Option | Drop Agent Option |
|--------------------|----------------|---------------------|----------------------|----------------------|-------------------|-------------------|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |

The statistics are described below.

Server Statistics

Transmit to Server: The number of packets that are relayed from client to server.

Transmit Error: The number of packets that resulted in errors while being sent to clients.

Receive from Server: The number of packets received from server.

Receive Missing Agent Option: The number of packets received without agent information options.

Receive Missing Circuit ID: The number of packets received with the Circuit ID option missing.

Receive Missing Remote ID: The number of packets received with the Remote ID option missing.

Receive Bad Circuit ID: The number of packets whose Circuit ID option did not match known circuit ID.

Receive Bad Remote ID: The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Transmit to Client: The number of relayed packets from server to client.

Transmit Error: The number of packets that resulted in error while being sent to servers.

Receive from Client: The number of received packets from server.

Receive Agent Option: The number of received packets with relay agent information option.

Replace Agent Option: The number of packets which were replaced with relay agent information option.

Keep Agent Option: The number of packets whose relay agent information was retained.

Drop Agent Option: The number of packets that were dropped which were received with relay agent information.

Buttons

Auto-refresh: Check this box to automatically refresh the page every three seconds.

Refresh: Click to refresh the page immediately.

Clear: Clear all statistics.

Monitor > DHCP > Detailed Statistics

The **Monitor > DHCP > Detailed Statistics** page displays the DHCP detailed statistics for the selected switch port for DHCP snooping. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. Also, clearing the statistics on a specific port may not take effect on global statistics since it gathers the different layer overview.

The screenshot shows the web interface for a Transition Networks S4224 Carrier Ethernet Network Interface Device. The page title is "DHCP Detailed Statistics Port 1". There are dropdown menus for "Combined" and "Port 1", and buttons for "Auto-refresh", "Refresh", and "Clear". The main content is a table with two columns: "Receive Packets" and "Transmit Packets".

| Receive Packets | | Transmit Packets | |
|-----------------------------|---|---------------------|---|
| Rx Discover | 0 | Tx Discover | 0 |
| Rx Offer | 0 | Tx Offer | 0 |
| Rx Request | 0 | Tx Request | 0 |
| Rx Decline | 0 | Tx Decline | 0 |
| Rx ACK | 0 | Tx ACK | 0 |
| Rx NAK | 0 | Tx NAK | 0 |
| Rx Release | 0 | Tx Release | 0 |
| Rx Inform | 0 | Tx Inform | 0 |
| Rx Lease Query | 0 | Tx Lease Query | 0 |
| Rx Lease Unassigned | 0 | Tx Lease Unassigned | 0 |
| Rx Lease Unknown | 0 | Tx Lease Unknown | 0 |
| Rx Lease Active | 0 | Tx Lease Active | 0 |
| Rx Discarded Checksum Error | 0 | | |
| Rx Discarded from Untrusted | 0 | | |

At the DHCP user select box, select the statistics to view:

Combined: all of the available DHCP statistics.

Normal Forward: only the normal forward statistics details.

Server: only the DHCP server statistics details.

Client: only the DHCP client statistics details.

Snooping: only the DHCP snooping statistics details.

Relay: only the DHCP relay statistics details.

The screenshot shows a dropdown menu with the following options: Combined (selected), Normal Forward, Server, Client, Snooping, and Relay.

The set of Combined statistics is summarized below.

| Receive Packets | Transmit Packets |
|-----------------------------|---------------------|
| Rx Discover | Tx Discover |
| Rx Offer | Tx Offer |
| Rx Request | Tx Request |
| Rx Decline | Tx Decline |
| Rx ACK | Tx ACK |
| Rx NAK | Tx NAK |
| Rx Release | Tx Release |
| Rx Inform | Tx Inform |
| Rx Lease Query | Tx Lease Query |
| Rx Lease Unassigned | Tx Lease Unassigned |
| Rx Lease Unknown | Tx Lease Unknown |
| Rx Lease Active | Tx Lease Active |
| Rx Discarded Checksum Error | |
| Rx Discarded from Untrusted | |

The DHCP Detailed Statistics parameters are described below.

Receive and Transmit Packets

Rx and Tx Discover

The number of discover (DHCP option 53 with value 1) packets received and transmitted.

Rx and Tx Offer

The number of offer (DHCP option 53 with value 2) packets received and transmitted.

Rx and Tx Request

The number of request (DHCP option 53 with value 3) packets received and transmitted.

Rx and Tx Decline

The number of decline (DHCP option 53 with value 4) packets received and transmitted.

Rx and Tx ACK

The number of ACK (DHCP option 53 with value 5) packets received and transmitted.

Rx and Tx NAK

The number of NAK (DHCP option 53 with value 6) packets received and transmitted.

Rx and Tx Release

The number of release (DHCP option 53 with value 7) packets received and transmitted.

Rx and Tx Inform

The number of inform (DHCP option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query

The number of lease query (DHCP option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned

The number of lease unassigned (DHCP option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown

The number of lease unknown (DHCP option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active

The number of lease active (DHCP option 53 with value 13) packets received and transmitted.

Rx Discarded checksum error

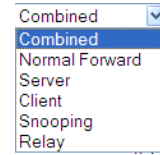
The number of discard packet that IP/UDP checksum is error.

Rx Discarded from Untrusted

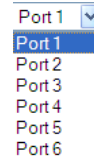
The number of discarded packet that are coming from untrusted port.

Buttons

The DHCP user select box determines which user is affected by clicking the buttons.



Port select box defines which port is affected by clicking the buttons.



Auto-refresh : Check this box to refresh the page automatically every three seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

DHCP Message Types

This option is used to convey the type of the DHCP message. The code for this option is 53, and its length is 1. Valid values for this option are:

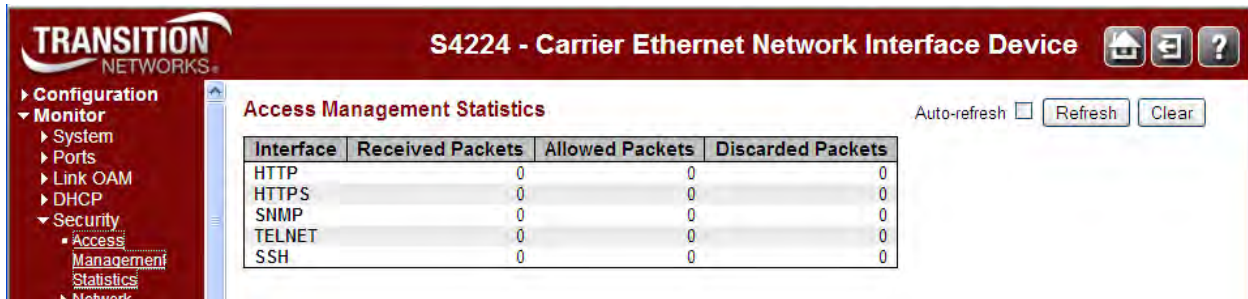
| Value | Message Type |
|-------|---------------|
| ----- | ----- |
| 1 | DHCP DISCOVER |
| 2 | DHCP OFFER |
| 3 | DHCP REQUEST |
| 4 | DHCP DECLINE |
| 5 | DHCP ACK |
| 6 | DHCP NAK |
| 7 | DHCP RELEASE |
| 8 | DHCP INFORM |

See <https://www.ietf.org/rfc/rfc2132.txt> for details.

Monitor > Security > Access Management

The **Monitor > Security > Access Management** Statistics menu path displays the Access Management Statistics table. This page provides statistics on the various S4224 access management interface methods.

The remote host can access the S4224 via HTTP, HTTPS, SNMP, TELNET, and/or SSH.



The screenshot shows the web interface for the S4224 Carrier Ethernet Network Interface Device. The page title is "S4224 - Carrier Ethernet Network Interface Device". The left navigation menu includes Configuration, Monitor, System, Ports, Link OAM, DHCP, Security, Access Management, Statistics, and Network. The main content area is titled "Access Management Statistics" and contains a table with the following data:

| Interface | Received Packets | Allowed Packets | Discarded Packets |
|-----------|------------------|-----------------|-------------------|
| HTTP | 0 | 0 | 0 |
| HTTPS | 0 | 0 | 0 |
| SNMP | 0 | 0 | 0 |
| TELNET | 0 | 0 | 0 |
| SSH | 0 | 0 | 0 |

Additional controls include an "Auto-refresh" checkbox, a "Refresh" button, and a "Clear" button.

The Access Management Statistics table parameters are explained below.

Interface

The interface type through which the remote host can access the S4224 (**HTTP**, **HTTPS**, **SNMP**, **TELNET**, and/or **SSH**).

Received Packets

Number of received packets from the interface when access management mode is enabled.

Allowed Packets

Number of allowed packets from the interface when access management mode is enabled.

Discarded Packets

Number of discarded packets from the interface when access management mode is enabled.

Buttons

Auto-refresh: Check this box to automatically refresh the page every three seconds.

Refresh: Click to refresh the page immediately.

Clear: Clear all statistics.

Monitor > Security > Network > Port Security

You can monitor the network device and ports' security from the **Monitor > Security > Network > Port Security** menu path.

Port Security > Switch

This page shows the current Port Security module and port status from the **Monitor > Security > Network > Port Security > Switch** menu path.

Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

Port Security Switch Status

Auto-refresh Refresh

User Module Legend

| User Module Name | Abbr |
|------------------|------|
| Limit Control | L |
| 802.1X | 8 |

Port Status

| Port | Users | State | MAC Count | |
|------|-------|----------|-----------|-------|
| | | | Current | Limit |
| 1 | -- | Disabled | - | - |
| 2 | -- | Disabled | - | - |
| 3 | -- | Disabled | - | - |
| 4 | -- | Disabled | - | - |
| 5 | -- | Disabled | - | - |
| 6 | -- | Disabled | - | - |
| 7 | -- | Disabled | - | - |
| 8 | -- | Disabled | - | - |

The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

User Module Legend

The legend shows all user modules that may request Port Security services.

User Module Name

The full name of a module that may request Port Security services.

Abbr

A one-letter abbreviation of the security user modules defined for the S4224 ports.

Limit Control - L

802.1X - 8

DHCP Snooping - D

The abbreviation is used in the 'Users' column in the Port Status table.

Port Status

The table has one row for each S4224 port and a number of columns. The columns are explained below.

Port

The port number for which the status applies. Click the linked port number to see the status for this particular port.

Users

Each of the user modules has a column that shows whether that module has enabled Port Security or not.

A '-----' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see '**Abbr**' description above) has enabled port security.

L- - - : Limit Control has enabled port security.

8 - - - : 802.1X has enabled port security.

D - - - : DHCP Snooping has enabled port security.

- - - - : the corresponding user module is not enabled.

State

Shows the current state of the port. It can take one of four values:

Disabled: No user modules are currently using the Port Security service.

Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.

Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

MAC Count (Current, Limit)

The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

If no user modules are enabled on the port, the Current column will show a dash (-).

If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this checkbox to automatically refresh the page every three seconds. .

Port Security > Port

In the **Port Status** section, when you click on a port in the table's Port column, the Port Security Port Status table displays for the specified S4224 port (e.g., Port 1 below). This page is also available from the **Monitor > Security > Network > Port Security > Port** menu path.

| MAC Address | VLAN ID | State | Time of Addition | Age/Hold |
|-------------------|---------|------------|---------------------------|----------|
| 00-04-75-bd-9c-36 | 1 | Forwarding | 1970-01-01T03:01:11+00:00 | 3221 |

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

MAC Address

The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.

VLAN ID

The VLAN ID that is seen on this port.

State

Indicates whether the corresponding MAC address is **Blocked** or **Forwarding**. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition

Shows the date and time when this MAC address was first seen on the port.

Age/Hold

If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Buttons

Port dropdown: Use the port select box () to select which port to show status for.

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to automatically refresh the page every three seconds.

Monitor > Security > Network > NAS

You can monitor the network NAS device and ports' security status from the **Monitor > Security > Network > NAS** menu path.

Network Access Server system and port configuration is done at the **Configuration > Security > Network > NAS** menu path (see page 94).

NAS > Switch

This page provides an overview of the current NAS ports' states.

| Port | Admin State | Port State | Last Source | Last ID | QoS Class | Port VLAN ID |
|------|------------------|-------------------|-------------|---------|-----------|--------------|
| 1 | Force Authorized | Globally Disabled | | | - | |
| 2 | Force Authorized | Globally Disabled | | | - | |
| 3 | Force Authorized | Globally Disabled | | | - | |
| 4 | Force Authorized | Globally Disabled | | | - | |
| 5 | Force Authorized | Globally Disabled | | | - | |
| 6 | Force Authorized | Globally Disabled | | | - | |
| 7 | Force Authorized | Globally Disabled | | | - | |
| 8 | Force Authorized | Globally Disabled | | | - | |
| 9 | Force Authorized | Globally Disabled | | | - | |
| 10 | Force Authorized | Globally Disabled | | | - | |
| 11 | Force Authorized | Globally Disabled | | | - | |
| 12 | Force Authorized | Globally Disabled | | | - | |
| 13 | Force Authorized | Globally Disabled | | | - | |
| 14 | Force Authorized | Globally Disabled | | | - | |

The NAS switch status parameters are explained below.

Port

Displays the S4224 port number. Click to display detailed NAS statistics for this port.

Admin State

Displays the port's current administrative state. If NAS is globally enabled, this selection controls the port's authentication mode.

Force Authorized: In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

Force Unauthorized: In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

Port-based 802.1X: In 802.1X, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs ([RFC3748](#)). Frames sent between the switch and the RADIUS server are **RADIUS** packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note: Suppose two backend servers are enabled and the server timeout is configured to *x* seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than *x* seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the *x* seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Single 802.1X: In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant.

Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X: Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant.

An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the 'Port Security Limit Control' functionality.

MAC-based Auth.: Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxx" (x is a hexadecimal digit). The switch only supports the [MD5-Challenge](#) authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is

supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

RADIUS-Assigned QoS Enabled: When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e., Port-based 802.1X or Single 802.1X.

RADIUS attributes used in identifying a QoS Class:

The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].

RADIUS-Assigned VLAN Enabled: When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e., Port-based 802.1X or Single 802.1X.

For troubleshooting VLAN assignments, use the "Monitor > VLANs > VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

RADIUS attributes used in identifying a VLAN ID:

RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

- The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.
- The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):
 - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).
 - Value of Tunnel-Type must be set to "VLAN" (ordinal 13).
 - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4094].

Guest VLAN Enabled: When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes, i.e.:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

For troubleshooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

Guest VLAN Operation:

When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

Port State

Displays the current state of the port. It can be one of the following values:

Globally Disabled: NAS is globally disabled at **Configuration > Security > Network > NAS > System Configuration > Mode = Disabled.**

Link Down: NAS is globally enabled, but there is no link on the port.

Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.

Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.

X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently, **X** clients are authorized and **Y** are unauthorized.

Last Source

Displays the source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

Last ID

Displays the user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

QoS Class

Displays the QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID

Displays the VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, " (RADIUS-assigned) " is appended to the VLAN ID. Read more about RADIUS-assigned VLANs.

If the port is moved to the Guest VLAN, " (Guest) " is appended to the VLAN ID.

Buttons

Refresh: Click to refresh the page immediately.

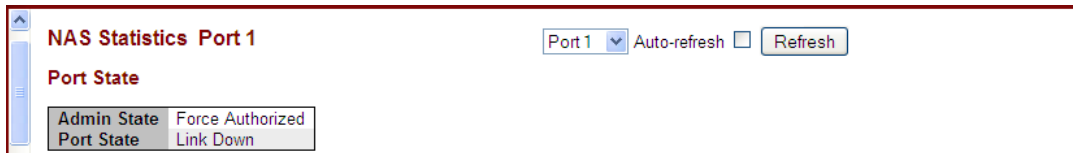
Auto-refresh: Check this checkbox to automatically refresh the page every 3 seconds.

NAS > Port

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows the selected backend server (e.g., RADIUS Authentication Server) statistics only.

Use the port select box () to select which port details to be displayed.

Depending on the current port state, the **Monitor > Security > Network > NAS > Port** menu path displays Port State data, or Port State and Port Counters data. The port state can be 'Globally Disabled', 'Link Down', or 'Authorized' as shown on the screen examples below.



The NAS Port State and Port Counters are explained below.

Admin State

Displays the the port's current administrative state. If NAS is globally enabled, this selection controls the port's authentication mode.

Force Authorized: In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

Force Unauthorized: In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

Port-based 802.1X: In 802.1X, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs ([RFC3748](#)). Frames sent between the switch and the RADIUS server are **RADIUS** packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch.

Single 802.1X: In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant.

Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X: Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant.

An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the 'Port Security Limit Control' functionality.

MAC-based Auth.: Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxx" (x is a hexadecimal digit). The switch only supports the [MD5-Challenge](#) authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

Port State

Displays the current state of the port. It can be one of the following values:

Globally Disabled: NAS is globally disabled at **Configuration > Security > Network > NAS > System Configuration > Mode = Disabled.**

Link Down: NAS is globally enabled, but there is no link on the port.

Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.

Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.

X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently, **X** clients are authorized and **Y** are unauthorized.

QoS Class

The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

Port VLAN ID

The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Port Counters

EAPOL Counters

These frame counters are available for these administrative states, as described in the table below: Force Authorized, Force Unauthorized, Port-based 802.1X, Single 802.1X, and Multi 802.1X.

Table 1. EAPOL Counters

| Direction | Name | IEEE Name | Description |
|-----------|-----------------------|---------------------------------|---|
| Rx | Total | dot1xAuthEapolFramesRx | The number of valid EAPOL frames of any type received by the S4224. |
| Rx | Response ID | dot1xAuthEapolRespIdFramesRx | The number of valid EAPOL Response Identity frames received by the S4224. |
| Rx | Responses | dot1xAuthEapolRespFramesRx | The number of valid EAPOL response frames (other than Response Identity frames) received by the S4224. |
| Rx | Start | dot1xAuthEapolStartFramesRx | The number of EAPOL Start frames that have been received by the switch. |
| Rx | Logoff | dot1xAuthEapolLogoffFramesRx | The number of valid EAPOL Logoff frames that have been received by the S4224. |
| Rx | Invalid Type | dot1xAuthInvalidEapolFramesRx | The number of EAPOL frames received by the S4224 in which the frame type is not recognized. |
| Rx | Invalid Length | dot1xAuthEapLengthErrorFramesRx | The number of EAPOL frames received by the S4224 in which the Packet Body Length field is invalid. |
| Tx | Total | dot1xAuthEapolFramesTx | The number of EAPOL frames of any type transmitted by the S4224. |
| Tx | Request ID | dot1xAuthEapolReqIdFramesTx | The number of EAPOL Request Identity frames transmitted by the S4224. |
| Tx | Requests | dot1xAuthEapolReqFramesTx | The number of valid EAPOL Request frames (other than Request Identity frames) transmitted by the S4224. |

Backend Server Counters

These backend (RADIUS) frame counters are available for the administrative states (Port-based 802.1X, Single 802.1X, Multi 802.1X, and MAC-based Auth.) as described in the table below.

Table 2. Backend Server Counters

| Direction | Name | IEEE Name | Description |
|-----------|--------------------------|---|---|
| Rx | Access Challenges | dot1xAuthBackendAccessChallenges | <p>802.1X-based: Counts the number of times the S4224 receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the S4224.</p> <p>MAC-based: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).</p> |
| Rx | Other Requests | dot1xAuthBackendOtherRequestsToSupplicant | <p>802.1X-based: Counts the number of times the S4224 sends an EAP Request packet following the first to the supplicant. Indicates the backend server chose an EAP-method.</p> <p>MAC-based: Not applicable.</p> |
| Rx | Auth. Successes | dot1xAuthBackendAuthSuccesses | <p>802.1X- and MAC-based: Counts the number of times the S4224 receives a success indication. Indicates the supplicant/client has successfully authenticated to the backend server.</p> |
| Rx | Auth. Failures | dot1xAuthBackendAuthFails | <p>802.1X- and MAC-based: Counts the number of times the S4224 receives a failure message. Indicates the supplicant/client has not authenticated to the backend server.</p> |
| Tx | Responses | dot1xAuthBackendResponses | <p>802.1X-based: Counts the number of times the S4224 attempts to send a supplicant's first response packet to the backend server. Indicates the S4224 attempted communication with the backend server. Possible retransmissions are not counted.</p> <p>MAC-based: Counts all the backend server packets sent from the S4224 towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.</p> |

Last Supplicant/Client Info

This field provides information about the last supplicant / client that attempted to authenticate (for the administrative states of Port-based 802.1X, Single 802.1X, Multi 802.1X, and MAC-based Auth.) as described in the table below.

Table 3. Last Supplicant/Client Information

| Last Supplicant/Client Info | | |
|-----------------------------|--------------------------------|--|
| Name | IEEE Name | Description |
| MAC Address | dot1xAuthLastEapolFrameSource | The MAC address of the last supplicant/client. |
| VLAN ID | --- | The VLAN ID on which the last frame from the last supplicant/client was received. |
| Version | dot1xAuthLastEapolFrameVersion | 802.1X-based: The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable. |
| Identity | --- | 802.1X-based: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. MAC-based: Not applicable. |

Selected Counters

Selected Counters

The Selected Counters table is visible when the port is in one of these administrative states:

- **Multi 802.1X**
- **MAC-based Auth.**

The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.

Attached MAC Addresses

Identity

Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it displays *No supplicants attached*. This column is not available for MAC-based Auth.

MAC Address

For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client. Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it displays *No clients attached*.

VLAN ID

The VLAN ID that the corresponding client is currently secured through the Port Security module.

State

The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend

server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for 'Hold Time 'seconds.

Last Authentication

Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Buttons



: Use the **Port select box** to select which port is affected when clicking the buttons:

Auto Refresh: Check this box to automatically refresh the page every three seconds.

Refresh: Click to refresh the page immediately.

Clear: Click to clear the counters for the selected port. This button is available in these modes:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X

Clear All: Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however. This button is available in the following modes:

- Multi 802.1X
- MAC-based Auth.X

Clear This: Click to clear only the currently selected client's counters. This button is available in these modes:

- Multi 802.1X
- MAC-based Auth.X

Monitor > Security > Network > ACL Status

You can display the current S4224 ACL Status table from the **Monitor > Security > Network > ACL Status** menu path.

This page shows the ACL status by the various ACL users. (The related configuration is done at the **Configuration > Security > Network > ACL** menu path.)

The screenshot shows the web interface for the S4224 Carrier Ethernet Network Interface Device. The page title is "S4224 - Carrier Ethernet Network Interface Device". The left sidebar shows a navigation menu with "Monitor" selected, and "Security" > "Network" > "ACL Status" highlighted. The main content area displays the "ACL Status" table. The table has columns for User, ACE, Frame Type, Action, Rate Limiter, CPU, Counter, and Conflict. The data is as follows:

| User | ACE | Frame Type | Action | Rate Limiter | CPU | Counter | Conflict |
|------|-----|------------|--------|--------------|-----|---------|----------|
| ptp | 1 | EType | Deny | Disabled | Yes | 0 | No |
| ptp | 2 | EType | Deny | Disabled | Yes | 0 | No |
| ptp | 4 | EType | Deny | Disabled | Yes | 0 | No |
| ptp | 3 | EType | Deny | Disabled | Yes | 0 | No |
| mep | 3 | EType | Deny | Disabled | No | 0 | No |
| mep | 2 | EType | Deny | Disabled | No | 0 | No |
| mep | 1 | EType | Permit | Disabled | Yes | 0 | No |

Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is **512** on each S4224.

User

Indicates the ACL user type (e.g., **dhcp**, **static**, **mep**, **ptp**, **evc**, **arp inspection**, **ip source Guard**).

ACE

Indicates the ACE ID on the local S4224.

Frame Type

Indicates the frame type of the ACE. The valid values are:

Any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. An Etype frame may be followed by a suffix such as '-0x88f7' or '-0x8902'.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.

IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.

IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.

IPv4/Other: The ACE will match IPv4 frames that are not ICMP/UDP/TCP.

IPv6: The ACE will match all IPv6 standard frames.

Action

Indicates the forwarding action of the ACE. **Permit** forwards packets if all other ACL criteria are met. **Deny** drops packets if all other ACL criteria is met.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Rate Limiter

Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When **Disabled** is displayed, the rate limiter operation is disabled.

CPU

Forward packet that matched the specific ACE to CPU.

Counter

The counter indicates the number of times the ACE was hit by a frame.

Conflict

Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons

: Select the ACL status from this drop down list. The selections are combined, static, ipManagement, ipSourceGuard, ipmc, evc, mep, arpInspection, upnp, ptp, dhcp, loopProtect, ttLoop, y1564, linkOam, ztp, and conflict. These selections are explained below.

combined: displays the ACL status of all of the selections (if any exist). This is the default.

static: displays the ACL status of just static ACL users.

ipManagement: displays the ACL status of just IP Management users.

ipSourceGuard: displays the ACL status of just the IP Source Guard users.

ipmc: displays the ACL status of just IPMC ACL users.

evc: displays the ACL status of just EVC ACL users.

mep: displays the ACL status of just MEP ACL users.

arpInspection: displays the ACL status of just the ARP Inspection ACL users.

upnp: displays the ACL status of just universal plug and play users.

ptp: displays the ACL status of just the PTP users.

dhcp: displays the ACL status of just the DHCP users.

loopProtect: displays the ACL status of just the loop protect mode users.

ttLoop: displays the ACL status of just the traffic test loop mode users.

y1564: displays the ACL status of just the Y.1564 users.

linkOam: displays the ACL status of just the Link OAM type ACL users.

ztp: displays the ACL status of just the zero touch provisioning users.

conflict: displays the ACL status of just conflicted ACL users.

```

combined
static
ipManagement
ipSourceGuard
ipmc
evc
mep
arpInspection
upnp
ptp
dhcp
loopProtect
ttLoop
y1564
linkOam
ztp
conflict

```

Auto-refresh: Check to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page; any changes made locally will be undone.

Examples

Static:

ACL Status Static

| User | ACE | Frame Type | Action | Rate Limiter | Mirror | CPU | Counter | Conflict |
|--------|-----|------------|--------|--------------|---------|-----|---------|----------|
| Static | 1 | IPv4 | Filter | 1 | Enabled | No | 0 | No |

MEP:

ACL Status MEP

| User | ACE | Frame Type | Action | Rate Limiter | Mirror | CPU | Counter | Conflict |
|------|-----|------------|--------|--------------|----------|-----|---------|----------|
| MEP | 6 | EType | Filter | Disabled | Disabled | No | 0 | No |
| MEP | 8 | EType | Filter | Disabled | Disabled | No | 0 | No |
| MEP | 1 | EType | Filter | Disabled | Disabled | No | 0 | No |
| MEP | 7 | EType | Filter | Disabled | Disabled | No | 0 | No |
| MEP | 2 | EType | Deny | Disabled | Disabled | Yes | 0 | No |
| MEP | 3 | EType | Deny | Disabled | Disabled | No | 0 | No |
| MEP | 4 | EType | Deny | Disabled | Disabled | Yes | 0 | No |
| MEP | 5 | EType | Deny | Disabled | Disabled | Yes | 0 | No |

PTP:

ACL Status PTP

| User | ACE | Frame Type | Action | Rate Limiter | Mirror | CPU | Counter | Conflict |
|------|-----|------------|--------|--------------|----------|-----|---------|----------|
| PTP | 1 | EType | Deny | Disabled | Disabled | Yes | 0 | No |
| PTP | 2 | EType | Deny | Disabled | Disabled | Yes | 0 | No |
| PTP | 3 | EType | Deny | Disabled | Disabled | Yes | 0 | No |
| PTP | 4 | EType | Deny | Disabled | Disabled | Yes | 0 | No |

Combined:

ACL Status combined

| User | ACE | Frame Type | Action | Rate Limiter | Mirror | CPU | Counter | Conflict |
|------|-----|------------|--------|--------------|----------|-----|---------|----------|
| mep | 10 | EType | Filter | Disabled | Disabled | No | 0 | No |
| mep | 9 | EType | Filter | Disabled | Disabled | No | 0 | No |
| mep | 8 | EType | Filter | Disabled | Disabled | No | 0 | No |
| mep | 7 | EType | Filter | Disabled | Disabled | No | 0 | No |
| mep | 6 | EType | Filter | Disabled | Disabled | No | 0 | No |
| mep | 1 | EType | Filter | Disabled | Disabled | No | 0 | No |
| mep | 2 | EType | Deny | Disabled | Disabled | Yes | 0 | No |
| mep | 3 | EType | Deny | Disabled | Disabled | No | 0 | No |
| mep | 4 | EType | Deny | Disabled | Disabled | Yes | 0 | No |
| mep | 5 | EType | Deny | Disabled | Disabled | Yes | 0 | No |
| evc | 501 | LLC | Deny | Disabled | Disabled | Yes | 0 | No |
| evc | 499 | EType | Deny | Disabled | Disabled | Yes | 0 | No |

Monitor > Security > Network > ARP Inspection

The **Monitor > Security > Network > ARP Inspection** menu path displays the Dynamic ARP Inspection Table.

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

The screenshot shows the web interface for the S4224 - Carrier Ethernet Network Interface Device. The left sidebar contains a navigation menu with the following items: Monitor, System, Ports, Link OAM, DHCP, Security (expanded), Access Management, Statistics, Network (expanded), Port Security, NAS, ACL Status, ARP Inspection (selected), and IP Source Guard. The main content area is titled "Dynamic ARP Inspection Table" and includes an "Auto-refresh" checkbox, a "Refresh" button, and navigation buttons for first, previous, next, and last entries. Below these are input fields for "Start from" (Port 1), "VLAN" (1), "MAC address" (00-00-00-00-00-00), and "IP address" (0.0.0.0), followed by an "entries per page" field set to 20. A table with columns "Port", "VLAN ID", "MAC Address", and "IP Address" is displayed, showing "No more entries".

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields let you select the starting point in the Dynamic ARP Inspection Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

Clicking the >> button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached, the text "*No more entries*" displays in the displayed table. Use the << button to start over.

The ARP Inspection table columns are explained below.

Port

Switch Port starting number for which the entries are displayed.

VLAN ID

VLAN-ID in which the ARP traffic is permitted.

MAC Address

User MAC address of the entry.

IP Address

User IP address of the entry.

Buttons

Auto-refresh: Check this checkbox to enable an automatic refresh of this page at 3 second intervals.

Refresh: Refreshes the displayed table starting from the input fields.

Clear: Flushes all dynamic entries.

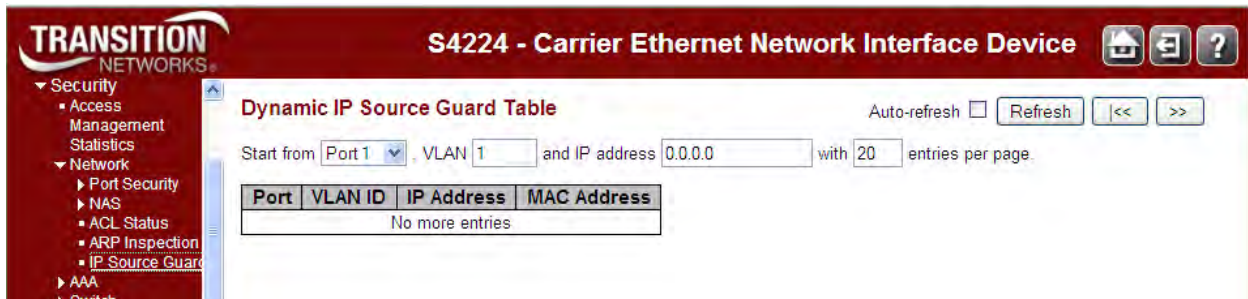
|<<: Updates the table starting from the first entry in the Dynamic ARP Inspection Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

Monitor > Security > Network > IP Source Guard

The **Monitor > Security > Network > IP Source Guard** menu path displays the Dynamic ARP Inspection Table.

The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.



Each page shows up to 99 entries from the Dynamic IP Source Guard table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic IP Source Guard Table.

The "Start from port address", "VLAN" and "IP address" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

Clicking the >> button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

The IP Source Guard Table columns are explained below.

Start from Port

Switch Port starting number for which the entries are displayed.

VLAN

The VLAN ID in which the IP traffic is permitted.

IP Address

The User IP address of the entry.

MAC Address

The Source MAC address.

Buttons

Auto-refresh: Check this checkbox to automatically refresh the page every three seconds. .

Refresh: Refreshes the displayed table starting from the input fields.

Clear: Flushes all dynamic entries.

|<<: Updates the table starting from the first entry in the Dynamic IP Source Guard Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

Monitor > Security > AAA

The **Monitor > Security > AAA** menu path provides RADIUS Overview and RADIUS Details data.

> RADIUS Overview

The RADIUS Authentication Overview page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page.

| # | IP Address | Authentication Port | Authentication Status | Accounting Port | Accounting Status |
|---|------------|---------------------|-----------------------|-----------------|-------------------|
| 1 | | | Disabled | | Disabled |
| 2 | | | Disabled | | Disabled |
| 3 | | | Disabled | | Disabled |
| 4 | | | Disabled | | Disabled |
| 5 | | | Disabled | | Disabled |

RADIUS Server Status Overview

#

The RADIUS server number. Click the linked number to navigate to detailed statistics for this server.

IP Address

The IP address of this server.

Port

The UDP port number for authentication.

Authentication Status

The current status of the server. This field takes one of the following values:

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Accounting Port

The UDP port number for accounting.

Accounting Status

The current status of the server. This field takes one of the following values:

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

> RADIUS Details

The **Monitor > Security > AAA > RADIUS Details** menu path provides detailed RADIUS Authentication Statistics for a particular RADIUS server.

The statistics map closely to those specified in [RFC4668 - RADIUS Authentication Client MIB](#).

Use the server select box to switch between the backend servers to show details for.

The screenshot displays the web interface for a Transition Networks S4224 Carrier Ethernet Network Interface Device. The left sidebar shows a navigation menu with 'RADIUS Details' selected under the 'Security' section. The main content area is titled 'RADIUS Authentication Statistics for Server #1' and includes a server selection dropdown set to 'Server #1', an 'Auto-refresh' checkbox, and 'Refresh' and 'Clear' buttons. Below this are two tables: 'RADIUS Authentication Statistics' and 'RADIUS Accounting Statistics'. Both tables have columns for 'Receive Packets' and 'Transmit Packets'. The authentication table shows metrics like Access Accepts, Access Rejects, Access Challenges, Malformed Access Responses, Bad Authenticators, Unknown Types, and Packets Dropped. The accounting table shows Responses, Malformed Responses, Bad Authenticators, Unknown Types, and Packets Dropped. Both tables also include an 'Other Info' section with IP Address, State (Disabled), and Round-Trip Time (0 ms).

RADIUS Authentication Statistics

Packet Counters

The RADIUS authentication server packet counters include seven receive counters and four transmit counters.

| Direction | Name | RFC4668 Name | Description |
|-----------|--------------------------|--------------------------------------|--|
| Rx | Access Accepts | radiusAuthClientExtAccess Accepts | The number of RADIUS Access-Accept packets (valid or invalid) received from the server. |
| Rx | Access Rejects | radiusAuthClientExtAccess Rejects | The number of RADIUS Access-Reject packets (valid or invalid) received from the server. |
| Rx | Access Challenges | radiusAuthClientExtAccess Challenges | The number of RADIUS Access-Challenge packets (valid or invalid) received from the server. |

| Direction | Name | RFC4668 Name | Description |
|-----------|-----------------------------------|---|---|
| Rx | Malformed Access Responses | radiusAuthClientExtMalformedAccessResponses | The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses. |
| Rx | Bad Authenticators | radiusAuthClientExtBadAuthenticators | The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server. |
| Rx | Unknown Types | radiusAuthClientExtUnknownTypes | The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped. |
| Rx | Packets Dropped | radiusAuthClientExtPacketsDropped | The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason. |
| Tx | Access Requests | radiusAuthClientExtAccessRequests | The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions. |
| Tx | Access Retransmissions | radiusAuthClientExtAccessRetransmissions | The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server. |
| Tx | Pending Requests | radiusAuthClientExtPendingRequests | The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission. |
| Tx | Timeouts | radiusAuthClientExtTimeouts | The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout. |

Other Info

This section contains information about the state of the server and the latest round-trip time.

| Name | RFC4668 Name | Description |
|------------------------|----------------------------------|--|
| IP Address | - | IP address and UDP port for the authentication server in question. |
| State | - | Shows the state of the server. It takes one of the following values: Disabled : The selected server is disabled. Not Ready : The server is enabled, but IP communication is not yet up and running. Ready : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left) : Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled. |
| Round-Trip Time | radiusAuthClientExtRoundTripTime | The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet. |

RADIUS Accounting Statistics

The statistics map closely to those specified in [RFC4670 - RADIUS Accounting Client MIB](#). Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS accounting server packet counter. There are five receive and four transmit counters.

| Direction | Name | RFC4670 Name | Description |
|-----------|----------------------------|--------------------------------------|--|
| Rx | Responses | radiusAccClientExtResponses | The number of RADIUS packets (valid or invalid) received from the server. |
| Rx | Malformed Responses | radiusAccClientExtMalformedResponses | The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses. |
| Rx | Bad Authenticators | radiusAcctClientExtBadAuthenticators | The number of RADIUS packets containing invalid authenticators received from the server. |
| Rx | Unknown Types | radiusAccClientExtUnknownTypes | The number of RADIUS packets of unknown types that were received from the server on the accounting |

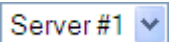
| Direction | Name | RFC4670 Name | Description |
|-----------|-------------------------|------------------------------------|---|
| | | | port. |
| Rx | Packets Dropped | radiusAccClientExtPackets Dropped | The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason. |
| Tx | Requests | radiusAccClientExtRequests | The number of RADIUS packets sent to the server. This does not include retransmissions. |
| Tx | Retransmissions | radiusAccClientExt Retransmissions | The number of RADIUS packets retransmitted to the RADIUS accounting server. |
| Tx | Pending Requests | radiusAccClientExtPending Requests | The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission. |
| Tx | Timeouts | radiusAccClientExtTimeouts | The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout. |

Other Info

This section contains information about the state of the server and the latest round-trip time.

| Name | RFC4670 Name | Description |
|------------------------|---------------------------------|--|
| IP Address | - | IP address and UDP port for the accounting server in question. |
| State | - | Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled. |
| Round-Trip Time | radiusAccClientExtRoundTripTime | The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet. |

Buttons

 The server select box determines which server is affected by clicking the buttons.

Auto-refresh: Check this box to automatically refresh the page every three seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

Monitor > Security > Switch > RMON

This page lets you display RMON (Remote Monitoring) statistics, history, alarms, and events. You configure RMON at the **Configuration > Security > Switch > RMON** menu path.

RMON > Statistics

This page provides an overview of RMON statistics entries (counters).

Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

The "Start from Control Index" allows the user to select the starting point in the Statistics table.

Clicking the **Refresh** button will update the displayed table starting from that or the next closest Statistics table match. The **>>** button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table.

Use the **|<<** button to start over.

TRANSITION NETWORKS+ S4224 - Carrier Ethernet Network Interface Device

RMON Statistics Status Overview

Auto-refresh Refresh |<< >>

Start from Control Index with entries per page.

| ID | Data Source (ifIndex) | Drop | Octets | Pkts | Broad-cast | Multi-cast | CRC Errors | Under-size | Over-size | Frag. | Jabb. | Coll. | 64 Bytes | 65 ~ 127 | 128 ~ 255 | 256 ~ 511 | 512 ~ 1023 | 1024 ~ 1688 |
|-----------------|-----------------------|------|--------|------|------------|------------|------------|------------|-----------|-------|-------|-------|----------|----------|-----------|-----------|------------|-------------|
| No more entries | | | | | | | | | | | | | | | | | | |

The displayed RMON statistics counters are explained below.

ID

Indicates the index of Statistics entry.

Data Source (ifIndex)

The data source which you want to be monitored.

Drop

The total number of events in which packets were dropped by the probe due to lack of resources.

Octets

The total number of octets of data (including those in bad packets) received on the network.

Pkts

The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broad-cast

The total number of good packets received that were directed to the broadcast address.

Multi-cast

The total number of good packets received that were directed to a multicast address.

CRC Errors

The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets.

Under-size

The total number of packets received that were less than 64 octets.

Over-size

The total number of packets received that were longer than 1518 octets.

Frag.

The number of frames with a size is less than 64 octets received with invalid CRC.

Jabb.

The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.

The best estimate of the total number of collisions on this Ethernet segment.

64 Bytes

The total number of packets (including bad packets) received that were 64 octets in length.

65~127

The total number of packets (including bad packets) received that were 65 to 127 octets in length.

128~255

The total number of packets (including bad packets) received that were 128 to 255 octets long.

256~511

The total number of packets (including bad packets) received that were 256 to 511 octets long.

512~1023

The total number of packets (including bad packets) received that were 512 to 1023 octets long.

1024~1588

The total number of packets (including bad packets) received that were 1024 to 1588 octets long.

Buttons

Auto-refresh: Check this box to automatically refresh the page every three seconds.

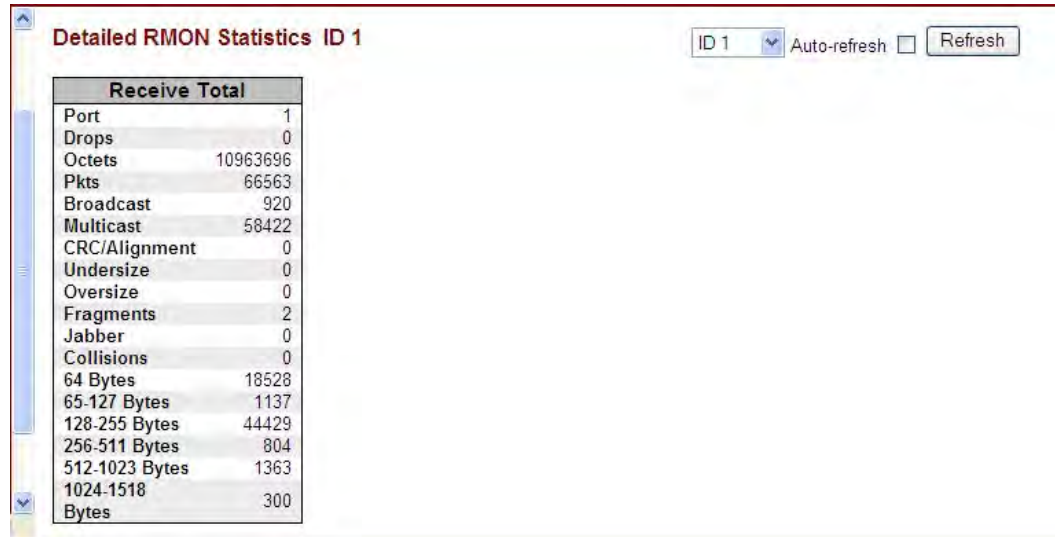
Refresh: Click to refresh the page immediately.

<<: Updates the table starting from the first entry in the Statistics table (i.e., the entry with the lowest ID).

>>: Updates the table, starting with the entry after the last entry currently displayed.


Detailed RMON Statistics

When you click an ID from the RMON Statistics Status Overview page, the “Detailed RMON Statistics” display for the selected instance.



| Receive Total | |
|-----------------|----------|
| Port | 1 |
| Drops | 0 |
| Octets | 10963696 |
| Pkts | 66563 |
| Broadcast | 920 |
| Multicast | 58422 |
| CRC/Alignment | 0 |
| Undersize | 0 |
| Oversize | 0 |
| Fragments | 2 |
| Jabber | 0 |
| Collisions | 0 |
| 64 Bytes | 18528 |
| 65-127 Bytes | 1137 |
| 128-255 Bytes | 44429 |
| 256-511 Bytes | 804 |
| 512-1023 Bytes | 1363 |
| 1024-1518 Bytes | 300 |

Buttons

ID 1 : Use the ID select dropdown box to select which port's detailed RMON statistics display.

Auto-refresh: Check this box to automatically refresh the page every three seconds.

Refresh: Click to refresh the page immediately.

|<<: Updates the table starting from the first entry in the Statistics table (i.e., the entry with the lowest ID).

>>: Updates the table, starting with the entry after the last entry currently displayed.

RMON > History

This page provides an overview of RMON history entries.

The RMON History Overview page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the **entries per page** input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

The **Start from History Index and Sample Index** lets you select the starting point in the History table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest History table match.

The **>>** button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "*No more entries*" is shown in the displayed table. Use the **|<<** button to start over.

| History Index | Sample Index | Sample Start | Drop | Octets | Pkts | Broad-cast | Multi-cast | CRC Errors | Under-size | Over-size | Frag. | Jabb. | Coll. | Utilization |
|---------------|--------------|--------------|------|---------|--------|------------|------------|------------|------------|-----------|-------|-------|-------|-------------|
| 1 | 1 | 6835163 | 0 | 6587088 | 101319 | 12 | 101033 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

The displayed fields are explained below.

History Index

Indicates the index of History control entry.

Sample Index

Indicates the index of the data entry associated with the control entry

Sample Start

The total number of events in which packets were dropped by the probe due to lack of resources.

Drops

The total number of events in which packets were dropped by the probe due to lack of resources.

Octets

The total number of octets of data (including those in bad packets) received on the network.

Pkts

The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast

The total number of good packets received that were directed to the broadcast address.

Multicast

The total number of good packets received that were directed to a multicast address.

CRC Errors

The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets.

Undersize

The total number of packets received that were less than 64 octets.

Oversize

The total number of packets received that were longer than 1518 octets.

Frag.

The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.

The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.

The best estimate of the total number of collisions on this Ethernet segment.

Utilization

The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent (.01% sampling interval).

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to automatically refresh the page every three seconds.

|<<: Updates the table starting from the first entry in the History table (i.e., the entry with the lowest History Index and Sample Index).

>>: Updates the table, starting with the entry after the last entry currently displayed.

RMON > Alarm

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table (the default is 20) as selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

The "Start from Control Index" allows the user to select the starting point in the Alarm table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Alarm table match.

The >> button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the << button to start over.

| ID | Interval | Variable | Sample Type | Value | Startup Alarm | Rising Threshold | Rising Index | Falling Threshold | Falling Index |
|----|----------|--------------------------|-------------|-------|-----------------|------------------|--------------|-------------------|---------------|
| 1 | 30 | .1.3.6.1.2.1.2.2.1.10.10 | Delta | 72 | RisingOrFalling | 2 | 2 | 1 | 1 |

The displayed fields are explained below.

ID

Indicates the index of Alarm control entry.

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

Variable

Indicates the particular variable to be sampled.

Sample Type

The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

Delta: Delta sampling subtracts the current sample value from the last sample taken and then compares the difference to the threshold. Delta sampling is like a counter that records a value that is constantly increasing. The difference between samples of the selected variable is used when comparing against the thresholds.

Absolute: Absolute sampling compares the sample value directly to the threshold. Absolute sampling is like a gauge that records values that go up or down. An actual value of the selected variable is used when comparing against the thresholds.

Value

The value of the statistic during the last sampling period. (e.g., **72**).

Startup Alarm

The alarm that may be sent when this entry is first set to valid (e.g., **RisingOrFalling**).

Rising Threshold

Rising threshold value.

Rising Index

Rising event index.

Falling Threshold

Falling threshold value.

Falling Index

Falling event index.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to automatically refresh the page every three seconds.

|<<: Updates the table starting from the first entry in the Alarm Table (i.e., the entry with the lowest ID).

>>: Updates the table, starting with the entry after the last entry currently displayed.

RMON > Event

The **Monitor > Security > Switch > RMON > Event** menu path displays the RMON Event Overview table.

This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table.

The "Start from Event Index and Log Index" lets you select the starting point in the Event table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Event table match. The **>>** button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "*No more entries*" is shown in the displayed table. Use the **|<<** button to start over.

The RMON Event Overview parameters are explained below.

Event Index

Indicates the index of the event entry.

LogIndex

Indicates the index of the log entry.

LogTime

Indicates the time that the Event was logged.

LogDescription

Indicates the Event description.

Buttons

Auto-refresh: Check this box to automatically refresh the page every three seconds.

Refresh: Click to refresh the page immediately.

|<<: Updates the table starting from the first entry in the Event Table (i.e., the entry with the lowest Event Index and Log Index).

>>: Updates the table, starting with the entry after the last entry currently displayed.

Monitor > LACP > System Status

The LACP System Status table displays from the **Monitor > LACP > System Status** menu path. This page provides a status overview of all LACP instances. Configuration is done from the **Configuration > Aggregation > LACP** menu path.

The **Monitor > LACP** menu path displays the System Status, Port Status, and Port Statistics sub-menus. LACP (Link Aggregation Control Protocol) is an IEEE 802.3ad standard protocol that allows bundling several physical ports together to form a single logical port. The message “*No ports enabled or no existing partners*” displays if no status is available.

The screenshot shows the web interface for the S4224 - Carrier Ethernet Network Interface Device. The left sidebar contains a navigation menu with 'Monitor' expanded to show 'System Status'. The main content area is titled 'LACP System Status' and features a table with the following columns: Aggr ID, Partner System ID, Partner Key, Partner Prio, Last Changed, and Local Ports. Below the table, the text 'No ports enabled or no existing partners' is displayed. To the right of the table, there is an 'Auto-refresh' checkbox (unchecked) and a 'Refresh' button.

The LACP System Status table parameters are explained below.

Aggr ID

The Aggregation ID associated with this aggregation instance. For LLAG (LACP Link Aggregation Groups) the ID is shown as 'isid:aggr-id' and for GLAGs (Global LAGs) as 'aggr-id'.

Partner System ID

The system ID (MAC address) of the aggregation partner.

Partner Key

The Key that the partner has assigned to this aggregation ID.

Partner Prio

The priority that the partner has assigned to this aggregation ID.

Last changed

The time since this aggregation changed.

Local Ports

Shows which ports are a part of this aggregation for this S4224.

Buttons

Refresh: Click to refresh this page immediately.

Auto-refresh: Check this checkbox to enable automatic refreshes of the page at 3 second intervals.

Monitor > LACP > Port Status

The LACP System Status table displays from the **Monitor > LACP > Port Status** menu path. This page provides a status overview for LACP status for all S4224 ports.

| Port | LACP | Key | Aggr ID | Partner System ID | Partner Port | Partner Prio |
|------|------|-----|---------|-------------------|--------------|--------------|
| 1 | No | - | - | - | - | - |
| 2 | No | - | - | - | - | - |
| 3 | No | - | - | - | - | - |
| 4 | No | - | - | - | - | - |
| 5 | No | - | - | - | - | - |
| 6 | No | - | - | - | - | - |
| 7 | No | - | - | - | - | - |
| 8 | No | - | - | - | - | - |
| 9 | No | - | - | - | - | - |

The LACP status table parameters are explained below.

Port

The S4224 port number for this row.

LACP

'Yes' means that LACP is enabled and the port link is up.

'No' means that LACP is not enabled or that the port link is down.

'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile its LACP status is disabled.

Key

The key assigned to this port. Displays a number from 1-65535. Only ports with the same key can aggregate together.

Aggr ID

The Aggregation ID assigned to this aggregation group.

Partner System ID

The partner's System ID (MAC address).

Partner Port

The partner's port number connected to this port.

Partner Prio

The partner's port priority.

Buttons

Refresh: Click to refresh this page immediately.

Auto-refresh: Check this box to automatically refresh the page every three seconds.

Monitor > LACP > Port Statistics

The LACP Statistics table displays from the **Monitor > LACP > Port Statistics** menu path.

This page provides an overview for LACP statistics for all ports.

The screenshot shows the web interface for the S4224 - Carrier Ethernet Network Interface Device. The left sidebar contains a navigation menu with 'Monitor' expanded to 'Port Statistics'. The main content area displays the 'LACP Statistics' table. Above the table are controls for 'Auto-refresh' (unchecked), 'Refresh', and 'Clear'.

| Port | LACP Received | LACP Transmitted | Discarded | |
|------|---------------|------------------|-----------|---------|
| | | | Unknown | Illegal |
| 1 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 |

The LACP Statistics table parameters are explained below.

Port

The S4224 port number.

LACP Received

Shows how many LACP frames have been received at each port.

LACP Transmitted

Shows how many LACP frames have been sent from each port.

Discarded

Shows how many Unknown and Illegal LACP frames have been discarded at each port.

Buttons


Auto-refresh: Check this box to enable an automatic refresh of this page at 3 second intervals.

Refresh: Click to refresh this page immediately.

Clear: Clears the counters for all ports.

Monitor > Loop Protection

The **Monitor > Loop Protection** menu path displays the loop protection port status of the S4224 ports in the form of the Loop Protection Status table.



| Port | Action | Transmit | Loops | Status | Loop | Time of Last Loop |
|------|--------------|----------|-------|--------|------|-------------------|
| 1 | Shutdown | Enabled | 0 | Up | - | - |
| 2 | Shutdown+Log | Enabled | 0 | Down | - | - |
| 3 | Log Only | Enabled | 0 | Down | - | - |
| 4 | Trap Only | Enabled | 0 | Down | - | - |
| 5 | Shut+Trap | Enabled | 0 | Up | - | - |
| 6 | Log+Trap | Enabled | 0 | Down | - | - |

Loop protection port status parameters are explained below.

Port

The S4224 port number of the logical port.

Action

The currently configured port action taken on loop detection:

Shutdown Port: Shutdown the port.

Shutdown + Log : Shutdown the port and Log the event.

Log Only: Only Log the event.

Trap Only: Only send a trap.

Shutdown + Trap: Shutdown the port and Send trap.

Log + Trap: Send a Trap and Log the event.

All: Shutdown the port, send a trap, and Log the event.

Transmit

The currently configured port transmit mode (Enabled or Disabled).

Loops

The number of loops detected on this port.

Status

The current loop protection status of the port (**Up** or **Down**).

Loop

Whether a loop is currently detected on the port.

Time of Last Loop

The time that the last loop event was detected.

Buttons

Auto-refresh: Check this box to automatically refresh the page every three seconds.

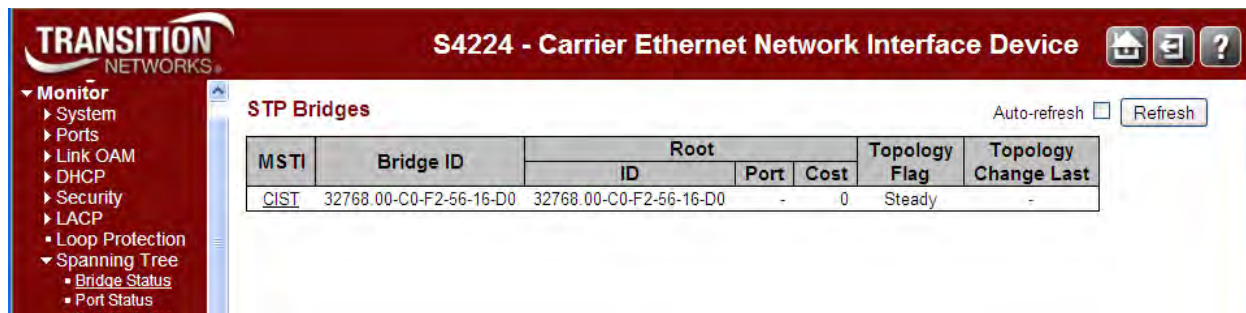
Refresh: Click to refresh the page immediately.

Monitor > Spanning Tree

The **Monitor > Spanning Tree** menu path displays the Bridge Status, Port Status, and Port Statistics sub-menus. Spanning tree protocols can include STP, MSTP, and RSTP.

Monitor > Spanning Tree > Bridge Status

The **Monitor > Spanning Tree > Bridge Status** menu path displays the STP Bridges table. This page provides a status overview of all STP bridge instances.



The screenshot shows the web interface for the S4224 - Carrier Ethernet Network Interface Device. The left sidebar contains a navigation menu with 'Monitor' expanded to show 'Spanning Tree' and its sub-items: 'Bridge Status', 'Port Status', and 'Port Statistics'. The main content area is titled 'STP Bridges' and includes an 'Auto-refresh' checkbox and a 'Refresh' button. Below this is a table with the following data:

| MSTI | Bridge ID | Root | | | Topology Flag | Topology Change Last |
|------|-------------------------|-------------------------|------|------|---------------|----------------------|
| | | ID | Port | Cost | | |
| CIST | 32768.00-C0-F2-56-16-D0 | 32768.00-C0-F2-56-16-D0 | - | 0 | Steady | - |

The table displays a row for each STP bridge instance; the column information is explained below.

MSTI

The Bridge Instance. This is also a link to the 'STP Detailed Bridge Status'. MSTP allows formation of MST regions that can run multiple MST instances (MSTI).

Bridge ID

The Bridge ID of this Bridge instance (e.g., *80:00:00:C0:F2:21:B8:C4*).

Root ID

The Bridge ID of the currently elected root bridge.

Root Port

The S4224 port currently assigned the *root* port role.

Root Cost

Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag

The current state of the Topology Change Flag of this Bridge instance (e.g., *Steady*).

Topology Change Last

The time since last Topology Change occurred.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to automatically refresh the page every three seconds.

Bridge Status Details

At **Monitor** > **Spanning Tree** > **Bridge Status** click on “**CIST**” in the MSTI column to display its details.

At **Monitor** > **Spanning Tree** > **Bridge Status** click on “**MISTIX**” in the MSTI column to display its details.

STP Detailed Bridge Status

| STP Bridge Status | |
|-----------------------|---------------------|
| Bridge Instance | CIST |
| Bridge ID | 0.00-C0-F2-56-1A-10 |
| Root ID | 0.00-C0-F2-56-19-98 |
| Root Cost | 20000 |
| Root Port | 4 |
| Regional Root | 0.00-C0-F2-56-1A-10 |
| Internal Root Cost | 0 |
| Topology Flag | Steady |
| Topology Change Count | 615 |
| Topology Change Last | 0d 01:06:52 |

CIST Ports & Aggregations State

| Port | Port ID | Role | State | Path Cost | Edge | Point-to-Point | Uptime |
|------|---------|---------------|------------|-----------|------|----------------|-------------|
| 4 | 240:004 | RootPort | Forwarding | 20000 | No | Yes | 0d 01:26:12 |
| 6 | 0:006 | AlternatePort | Discarding | 20000 | No | Yes | 0d 01:27:27 |

The **STP Detailed Bridge Status** table parameters are described below with sample values.

Bridge Instance

The Bridge instance (e.g., **MSTI1** or **CIST**).

Bridge ID

The Bridge ID of this Bridge instance (e.g., **80:01-00:C0:F2:00:00:01** or **32768.00-C0-F2-56-1A-90**).

Root ID

The Bridge ID of the currently elected root bridge (e.g., **80:01-00:C0:F2:00:00:01** or **32768.00-C0-F2-56-1A-90**).

Root Cost

Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge (e.g., **0**, **20000**).

Root Port

The switch port currently assigned the root port role (e.g., **-** indicating none reported).

Regional Root

The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge (e.g., **80:00-00:C0:F2:00:00:01** or **32768.00-C0-F2-56-1A-90**) (displays for CIST only).

Internal Root Cost

The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge (e.g., **0**) (displays for CIST only).

Topology Flag

The current state of the Topology Change Flag of this Bridge instance (e.g., **Steady**).

Topology Change Count

The number of times the topology change flag has been set (during a one-second interval) (e.g., **0**).

Topology Change Last

The time passed since the Topology Flag was last set (e.g., **0d 01:15:55**, or **-** indicating none encountered).

The **CIST Ports & Aggregations State** table parameters are shown below with sample parameters.

CIST Ports & Aggregations State

| Port | Port ID | Role | State | Path Cost | Edge | Point2Point | Uptime |
|------|---------|----------------|------------|-----------|------|-------------|-------------|
| 1 | 128-001 | DesignatedPort | Forwarding | 200000 | Yes | Yes | 0d 01:15:53 |
| 5 | 128-005 | DesignatedPort | Forwarding | 20000 | No | Yes | 0d 01:15:56 |

Port

The switch port number of the logical STP port (e.g., **1**).

Port ID

The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port (e.g., **128:009**).

Role

The current STP port role. The port role can be **AlternatePort**, **BackupPort**, **RootPort**, or **DesignatedPort**.

State

The current STP port state. The port state can be **Discarding**, **Learning**, or **Forwarding**.

Path Cost

The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value (e.g., **200000**).

Edge

The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop (e.g., **Yes** or **No**).

Point2Point

The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state. (e.g., **Yes** or **No**)

Uptime

The time since the bridge port was last initialized (e.g., **0d 03:54:57**).
If nothing is configured, displays the message "*No ports or aggregations active*" displays.

Monitor > Spanning Tree > Port Status

The **Monitor > Spanning Tree > Port Status** menu path displays the STP Port Status table, which provides the STP CIST port status for the S4224 physical ports.

An MSTn instance is local to a region. ISTs in different regions are interconnected via a Common Spanning Tree (CST). The Common and Internal Spanning Tree (CIST) includes the collection of ISTs in each MST region, and the CST that connects the ISTs.

As a result of the spanning-tree calculation, ports will assume various roles in the topology. A root port is a port facing towards the root that is connected to the 'best path' back to the root. 'Best path' means:

- 1) the path with the lowest cost back to the root,
- 2) the path going through the device with the lowest BID if there is more than device advertising the lowest cost, and
- 3) the lowest port ID on that device if there is more than one connection to the device.

| Port | CIST Role | CIST State | Uptime |
|------|-----------|------------|--------|
| 1 | Disabled | Discarding | - |
| 2 | Disabled | Discarding | - |
| 3 | Disabled | Discarding | - |
| 4 | Disabled | Discarding | - |
| 5 | Disabled | Discarding | - |
| 6 | Disabled | Discarding | - |
| 7 | Disabled | Discarding | - |
| 8 | Disabled | Discarding | - |
| 9 | Disabled | Discarding | - |
| 10 | Disabled | Discarding | - |
| 11 | Disabled | Discarding | - |

The STP Port Status table parameters are explained below.

Port

The S4224 port number of the logical STP port.

CIST Role

The current STP port role of the CIST port. The port role value can be:

AlternatePort: An alternative path to the root bridge. This path is different than using the root port.

BackupPort: A backup/redundant path to a segment where another bridge port already connects.

RootPort: Port by which frames leave a device to reach the root (forwarding port). This refers to a forwarding port that is the best port from Nonroot-bridge to Rootbridge.

DesignatedPort: Port by which frames enter a device to reach the root (forwarding port). A forwarding port for every LAN segment. A Non-Designated port is a Port blocking frames to prevent a loop in the topology (blocking port).

Disabled: Not strictly part of STP, a network administrator can manually disable a port.

Non-STP: the port is not STP-capable.

CIST State

The current STP port state of the CIST port. The port state can be one of the following values: **Learning**, **Forwarding**, **Discarding**.

STP per IEEE 802.1d proceeds through various states to establish the topology.

Learning: After the Blocking state, ports then enter a Learning phase where they listen to frames reaching their ports to build the MAC tables on the device. While the port does not yet forward frames (packets) it does learn source addresses from frames received and adds them to the filtering database (switching database).

Forwarding: After the Learning state, the root and designated ports enter the Forwarding state, while the non-designated ports are set to blocking state. A port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.

Discarding: The device is discarding all non-OAMPDUs.

RSTP switch port states include Discarding (no user data is sent over the port), Learning (the port is not forwarding frames yet, but is populating its MAC-address-table), and Forwarding (the port is fully operational).

Uptime

The time since the bridge port was last initialized (e.g., **9d 04:09:48**, or 9 days, 4 hours, 9 minutes and 48 seconds).

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this checkbox to enable automatic page refreshes at 3 second intervals.

Monitor > Spanning Tree > Port Statistics

The **Monitor > Spanning Tree > Port Statistics** menu path displays the STP Port Status table, which provides the STP port statistics counters of S4224 bridge ports. STP statistics are provided for STP, MSTP, and RSTP.

| Port | Transmitted | | | | Received | | | | Discarded | |
|------|-------------|------|-----|-----|----------|------|-----|-----|-----------|---------|
| | MSTP | RSTP | STP | TCN | MSTP | RSTP | STP | TCN | Unknown | Illegal |
| 1 | 6455 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

The STP port Statistics counters are explained below.

Port

The S4224 port number of the logical STP port.

MSTP

The number of MSTP Configuration BPDUs received/transmitted on the port. The Multiple Spanning Tree Protocol (MSTP) allows formation of MST regions that can run multiple MST instances (MSTI). Multiple regions and other STP bridges are interconnected using one single common spanning tree (CST).

RSTP

The number of RSTP Configuration BPDUs received/transmitted on the port. IEEE document 802.1w introduced RSTP as an evolution of STP. The Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now uses RSTP and obsoletes STP, while at the same time remains backwards compatible with STP.

STP

The number of legacy STP Configuration BPDUs received/transmitted on the port. The Spanning Tree Protocol (STP, per IEEE 802.1D) creates a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches), and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes.

TCN

The number of (legacy) Topology Change Notification (TCN) BPDUs received/transmitted on the port. TCN BPDUs are used to inform other devices of port changes. TCNs are injected into the network by a non-root switch and propagated to the root. On receipt of the TCN, the root switch will set a Topology Change flag in its normal BPDUs. This flag is propagated to all other switches to instruct them to rapidly age out their forwarding table entries.

Discarded Unknown

The number of unknown Spanning Tree BPDUs received (and discarded) on the port.

Discarded Illegal

The number of illegal Spanning Tree BPDUs received (and discarded) on the port.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this checkbox to enable automatic page refreshes at 3 second intervals.

Clear: Click to reset the counters.

Monitor > MVR

You can view Statistics, MVR Channel Groups, and MVR SFM Information from the **Monitor > MVR** menu path. MVR is configured from the **Configuration > MVR** menu path.

Statistics

This page provides MVR Statistics information from the **Monitor > MVR > Statistics** menu path.

| MVR Statistics | | | | | | |
|----------------|---------------------------|------------------------------|-----------------------|-------------------------------|-------------------------------|------------------------------|
| VLAN ID | IGMP/MLD Queries Received | IGMP/MLD Queries Transmitted | IGMPv1 Joins Received | IGMPv2/MLDv1 Reports Received | IGMPv3/MLDv2 Reports Received | IGMPv2/MLDv1 Leaves Received |
| 10 | 0 / 0 | 0 / 0 | 0 | 0 / 0 | 0 / 0 | 0 / 0 |
| 20 | 0 / 0 | 0 / 0 | 0 | 0 / 0 | 0 / 0 | 0 / 0 |

The MVR Statistics information is explained below.

VLAN ID

The Multicast VLAN ID.

IGMP/MLD Queries Received

The number of Received Queries for IGMP and MLD, respectively.

IGMP/MLD Queries Transmitted

The number of Transmitted Queries for IGMP and MLD, respectively.

IGMPv1 Joins Received

The number of Received IGMPv1 Joins.

IGMPv2/MLDv1 Reports Received

The number of Received IGMPv2 Joins and MLDv1 Reports, respectively.

IGMPv3/MLDv2 Reports Received

The number of Received IGMPv1 Joins and MLDv2 Reports, respectively.

IGMPv2/MLDv1 Leaves Received

The number of Received IGMPv2 Leaves and MLDv1 Dones, respectively.

Buttons

Auto-refresh: Automatic refresh occurs every three seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears all Statistics counters.

MVR Channel Groups

This page provides MVR Channel (Groups) information from the **Monitor > MVR > MVR Channel Groups** menu path. Entries in the MVR Channels (Groups) Information Table are shown on this page. The MVR Channels (Groups) Information Table is sorted first by VLAN ID, and then by group.

The screenshot shows the web interface for the S4224 Carrier Ethernet Network Interface Device. The main content area is titled "MVR Channels (Groups) Information". It includes an "Auto-refresh" checkbox, a "Refresh" button, and navigation buttons for first, previous, next, and last. Below these are input fields for "Start from VLAN" (set to 1) and "Group Address" (empty), followed by "with 20 entries per page". A table titled "Port Members" has columns for "VLAN ID" and "Groups", and 28 numbered columns for ports. The table currently displays "No more entries".

Each page shows up to 99 entries from the MVR Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Channels (Groups) Information Table.

The "Start from VLAN", and "Group Address" input fields let you select the starting point in the MVR Channels (Groups) Information table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MVR Channels (Groups) Information table match. In addition, the two input fields will - upon a >> button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" displays in the table. Use the |<< button to start over.

The MVR Channel (Groups) information is explained below.

Group Address

The IPv4 / IPv6 address of the group (e.g., IPv4 multicast addresses range 224.0.0.0 to 239.255.255.255).

VLAN ID

The VLAN ID of the group.

Groups

The Group ID of the group displayed.

Port Members

Ports under this group.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the input fields.

|<<: Updates the table starting from the first entry in the MVR Channels (Groups) Information Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

MVR SFM Information

This page provides MVR Channel (Groups) information from the **Monitor > MVR > MVR SFM Information** menu path.

The MVR SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Each page shows up to 99 entries from the MVR SFM Information Table (default is 20) selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR SFM Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR SFM Information table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MVR SFM Information Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

The MVR SFM (Source-Filtered Multicast) Information table entries are explained below.

Group Address

The IPv4 / IPv6 address of the group (e.g., IPv4 multicast addresses range 224.0.0.0 to 239.255.255.255).

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port

Switch port number.

Mode

Indicates the filtering mode maintained per (VLAN ID, Port number, Group Address) basis. Mode can be set to either **Include** or **Exclude**.

Source Address

The IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no any source filtering address, the text "None" displays in the Source Address field.

Type

Indicates the type of MVR performed. It can be either **Allow** or **Deny**.

Hardware Filter/Switch

Indicates whether the data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by the chip.

Buttons

Auto-refresh: Check the checkbox to cause an automatic refresh to occur every 3 seconds.

Refresh: Refreshes the displayed table starting from the input fields.

|<<: Updates the table starting from the first entry in the MVR SFM Information table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

Monitor > IPMC > IGMP Snooping

The **Monitor > IPMC > IGMP Snooping** menu path provides the Status, Groups Information, and IPv4 SFM Information sub-menus.

The IGMP (Internet Group Management Protocol) communications protocol is used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP allows more efficient use of resources when supporting uses such as online video.

IGMP Snooping Status

This page provides IGMP Snooping status in terms of statistics and router port status.

The screenshot shows the 'IGMP Snooping Status' page. The 'Statistics' table is as follows:

| VLAN ID | Querier Version | Host Version | Querier Status | Queries Transmitted | Queries Received | V1 Reports Received | V2 Reports Received | V3 Reports Received | V2 Leave Receiv |
|---------|-----------------|--------------|----------------|---------------------|------------------|---------------------|---------------------|---------------------|-----------------|
| 1 | | | | | | | | | |
| 2 | | | | | | | | | |
| 3 | | | | | | | | | |
| 4 | | | | | | | | | |
| 5 | | | | | | | | | |
| 6 | | | | | | | | | |
| 7 | | | | | | | | | |
| 8 | | | | | | | | | |
| 9 | | | | | | | | | |
| 10 | | | | | | | | | |
| 11 | | | | | | | | | |

The 'Router Port' table is as follows:

| Port | Status |
|------|--------|
| 1 | - |
| 2 | - |
| 3 | - |
| 4 | - |
| 5 | - |
| 6 | - |
| 7 | - |
| 8 | - |
| 9 | - |
| 10 | - |
| 11 | - |

The IPMC Snooping status **Statistics** information is explained below.

VLAN ID

The VLAN ID of the entry (e.g., VLAN ID 1).

Querier Version

The working Querier Version currently in use (e.g., **v3** shown above). In order for IGMP, and IGMP snooping, to function, a multicast router must exist on the network and generate IGMP queries. The tables created for snooping that (hold the member ports for a multicast group) are associated with the querier. Without a querier, the tables are not created and snooping does not work. IGMP general queries must be unconditionally forwarded by all switches involved in IGMP snooping.

Host Version

The working Host Version currently in use (e.g., **v3** shown above).

Three versions of IGMP exist - versions **v1**, **v2**, and **v3**. One difference between the versions is how a host node signals that it no longer wants to be a member of a multicast group.

In **v1**, the host node stops sending reports. If a router does not receive a report from a host node after a predefined length of time (time-out value) it assumes that the host node no longer wants to

receive multicast frames and removes it from the membership list of the multicast group. In v2, a host node exits from a multicast group by sending a leave request. After receiving a leave request from a host node, the router removes the node from appropriate membership list. The router also stops sending multicast packets from the port if it determines there are no further host nodes on the port.

v3 adds the ability of host nodes to "join" or "leave" specific sources in a multicast group.

IGMP support in Microsoft Windows hosts includes:

IGMPv1 in Windows 95, Windows NT 4.0 (SP3 and earlier).

IGMPv2 in Windows 98, Windows ME, Windows NT 4.0 (SP4 and later), Windows 2000.

IGMPv3 in Windows XP, Windows Server 2003, Windows Vista.

For more information see <http://support.microsoft.com/>.

Querier Status

Displays the Querier status as "ACTIVE" or "IDLE".

Queries Transmitted

The number of Transmitted Queries (e.g., 5).

Queries Received

The number of Received Queries.

V1 Reports Received

The number of Received V1 Reports.

V2 Reports Received

The number of Received V2 Reports.

V3 Reports Received

The number of Received V3 Reports.

V2 Leaves Received

The number of Received V2 Leaves.

The IPMC Snooping status table **Router Port** information is explained below. Displays which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

Port

The S4224 port number.

Status

Indicate whether a specific port is a router port. The IGMP Snooping status Router Port table display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

static denotes the specific port is configured to be a router port.

dynamic denotes the specific port is learnt to be a router port.

both denote the specific port is configured or learnt to be a router port.

-- indicates there is no status to display.

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clears all Statistics counters.

Auto-refresh: Check this checkbox to enable automatic page refreshes at 3 second intervals.

IGMP Snooping > Groups Information

Entries in the IGMP Group Table are displayed on this page. The IGMP Group Table is sorted first by VLAN ID, and then by Group.

The screenshot shows the web interface for the S4224 - Carrier Ethernet Network Interface Device. The main content area is titled "IGMP Snooping Group Information". It features an "Auto-refresh" checkbox (unchecked), a "Refresh" button, and navigation buttons for first and last entries. Below this, there are input fields for "Start from VLAN" (set to 1) and "group address" (set to 224.0.0.0), followed by a field for "entries per page" (set to 20). A table titled "Port Members" is displayed, with columns for "VLAN ID" and "Groups". The table content shows "No more entries".

| | | Port Members | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------|--------|-----------------|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| VLAN ID | Groups | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| | | No more entries | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Each page shows up to 99 entries from the IGMP Group table selected through the "entries per page" input field (the default is 20). When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

The "Start from VLAN", and "group address" input fields let you select the starting point in the IGMP Group Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. They will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

VLAN ID

VLAN ID of the IGMP group.

Groups

Group address of the IGMP group displayed.

Port Members

Ports under this IGMP group.

Buttons

Auto-refresh: Check this checkbox to automatically refresh the page every three seconds. .

Refresh: Refreshes the displayed table starting from the input fields.

|<<: Updates the table, starting with the first entry in the IGMP Group table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

IGMP Snooping IPv4 SFM Information

Entries in the IGMP SFM Information table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Each page shows up to 99 entries from the IGMP SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, this page shows the first 20 entries from the beginning of the IGMP SFM Information table.

The "Start from VLAN", and "Group" input fields allow the user to select the starting point in the IGMP SSM Information Table. Clicking **Refresh** the button will update the displayed table starting from that or the closest next IGMP SFM Information table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "*No more entries*" displays in the displayed table. Use the << button to start over.

VLAN ID

VLAN ID of the group (e.g., **VLAN ID 1**).

Group

Group address of the group displayed (e.g., **239.255.255.250**).

Port

S4224 port number.

Mode

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either '**Include**' or '**Exclude**'.

Source Address

The IP Address of the source. Currently, the maximum number of IPv4 source address for filtering (per group) is **8**. When there is no source filtering address, the text "**None**" is shown in the Source Address field.

Type

Indicates the Type. It can be either '**Allow**' or '**Deny**'.

Hardware Filter/Switch

Indicates whether the data plane destined to the specific group address from the source IPv4 address could be handled by the chip.

Buttons

Auto-refresh: Check this box to automatically refresh the page every three seconds.

Refresh: Refreshes the displayed table starting from the input fields.

|<<: Updates the table starting from the first entry in the IGMP SSM Information Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

Monitor > IPMC > MLD Snooping

The **Monitor > IPMC > MLD Snooping** menu path provides the Status, Groups Information, and IPv6 SSM Information sub-menus. MLD (Multicast Listener Discovery) for IPv6 is used by IPv6 routers to discover multicast listeners on a directly-attached link (much as IGMP is used in IPv4). The MLD protocol is embedded in ICMPv6 instead of using a separate protocol.

MLD Snooping > Status

The **MLD Snooping > Status** page provides MLD Snooping status.

The screenshot shows the web interface for a Transition Networks S4224 Carrier Ethernet Network Interface Device. The page title is 'MLD Snooping Status'. There are 'Auto-refresh' (unchecked), 'Refresh', and 'Clear' buttons. The 'Statistics' table is as follows:

| VLAN ID | Querier Version | Host Version | Querier Status | Queries Transmitted | Queries Received | V1 Reports Received | V2 Reports Received | V1 Leaves Received |
|---------|-----------------|--------------|----------------|---------------------|------------------|---------------------|---------------------|--------------------|
| 1 | | | | | | | | |
| 2 | | | | | | | | |
| 3 | | | | | | | | |
| 4 | | | | | | | | |
| 5 | | | | | | | | |
| 6 | | | | | | | | |
| 7 | | | | | | | | |
| 8 | | | | | | | | |
| 9 | | | | | | | | |
| 10 | | | | | | | | |
| 11 | | | | | | | | |

The 'Router Port' table is as follows:

| Port | Status |
|------|--------|
| 1 | - |
| 2 | - |
| 3 | - |
| 4 | - |
| 5 | - |
| 6 | - |
| 7 | - |
| 8 | - |
| 9 | - |
| 10 | - |
| 11 | - |

The MLD Snooping Status table **Statistics** parameters are explained below.

VLAN ID

The VLAN ID of the entry (e.g., VLAN ID 1 shown above).

Querier Version

The working Querier Version currently (e.g., **v2** shown above).

Host Version

The working Host Version currently in use (e.g., **v2** shown above).

MLD **v1** was the original release of MLD as an asymmetric protocol, specifying different behaviors for multicast listeners and for routers per IETF [RFC 2710](#).

MLD**v2** is designed to be interoperable with MLDv1. MLDv2 adds the ability for a node to report interest in listening to packets with a particular multicast address only from specific source addresses or from all sources except for specific source addresses. Refer to IETF [RFC 3810](#).

Windows support includes:

MLDv1 in Windows 98, Windows ME, Windows NT 4.0 (SP4 and later), Windows 2000.

MLDv2 in Windows XP, Windows Server 2003, Windows Vista.

Windows XP supports the host side of MLDv1 and can function as a multicast source or receiver. Multicast routing support is not present on XP.

IPv6 in Windows Server 2008 and Windows Vista supports both MLD and MLDv2.

IPv6 in Windows Server 2008 and Windows Vista uses MLDv2 by default, but will use MLD if it receives an MLD message. You can configure IPv6 to use MLD with the “**netsh interface ipv6 set global mldversion=version2**” command.

Querier Status

Shows the Querier status as “**ACTIVE**” or “**IDLE**”. The status “**DISABLE**” means the specific interface is administratively disabled.

Queries Transmitted

The number of Transmitted Queries.

Queries Received

The number of Received Queries.

V1 Reports Received

The number of Received V1 Reports.

V2 Reports Received

The number of Received V2 Reports.

V1 Leaves Received

The number of Received V1 Leaves.

The MLD Snooping Status table **Router Port** parameters are explained below.

Router Port

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

static denotes the specific port is configured to be a router port.

dynamic denotes the specific port is learnt to be a router port.

both denote the specific port is configured or learnt to be a router port.

Port

S4224 port number.

Status

Indicate whether or not a specific port is a router port.

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clears all Statistics counters.

Auto-refresh: Check this box to automatically refresh the page every three seconds.

MLD Snooping > Groups Information

The **MLD Snooping > Groups Information** menu path displays entries in the MLD Group Table. The MLD Groups Table is sorted first by VLAN ID, and then by group.

The screenshot shows the web interface for MLD Snooping Group Information. The page title is "S4224 - Carrier Ethernet Network Interface Device". The main heading is "MLD Snooping Group Information". Below the heading, there are input fields for "Start from VLAN" (set to 1) and "group address" (set to ff00:), and a "Refresh" button. A table titled "Port Members" is displayed, with columns for "VLAN ID" and "Groups" (1-28). The table content is empty, displaying "No more entries".

Each page shows up to 99 entries from the MLD Group table selected through the "**entries per page**" input field (the default is 20). When first visited, the web page will show the first 20 entries from the beginning of the MLD Group Table.

The "Start from VLAN", and "group address" input fields let you select the starting point in the MLD Group Table. Click the **Refresh** button to update the displayed table starting from that or the next closest MLD Group Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The **>>** will use the last entry of the currently displayed as a basis for the next lookup. When the end is reached the text "*No more entries*" is shown in the displayed table. Use the **|<<** button to start over.

The **MLD Snooping > Groups Information** parameters are explained below.

VLAN ID

The VLAN ID of the entry (e.g., VLAN ID 1).

Groups

Group address of the group displayed.

Port Members

Ports under this group.

Buttons

Auto-refresh: Check this checkbox to automatically refresh the page every three seconds. .

Refresh: Refreshes the displayed table starting from the input fields.

|<<: Updates the table starting from the first entry in the MLD Group Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

MLD Snooping > IPv6 SFM Information

The **MLD Snooping > IPv6 SFM Information** menu path displays entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

Each page shows up to 99 entries from the MLD SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD SFM Information Table.

The "Start from VLAN", and "Group" input fields allow the user to select the starting point in the MLD SFM Information table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MLD SFM Information table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The **>>** button will use the last entry of the currently displayed as a basis for the next lookup. When the end is reached, the text "*No more entries*" displays in the displayed table. Use **<<** the button to start over.

VLAN ID

VLAN ID of the group.

Group

The Group address of the group displayed (e.g., `ff02::1:ff00:108`).

Port

The S4224 port number.

Mode

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either **'Include'** or **'Exclude'**.

Source Address

The IP Address of the source. Currently, the maximum number of IPv6 source address for filtering (per group) is 8. When there is no any source filtering address, the text "None" is shown in the Source Address field.

Type

Indicates the type of action. It can be either **'Allow'** or **'Deny'**.

Hardware Filter/Switch

Indicates whether the data plane destined to the specific group address from the source IPv6 address could be handled by the chip.

Buttons

Auto-refresh: Check this box to automatically refresh the page every three seconds.

Refresh: Refreshes the displayed table starting from the input fields.

|<<: Updates the table starting from the first entry in the MLD SSM Information Table.

>>: Updates the table, starting with the entry after the last entry currently displayed.

Monitor > LLDP

The **Monitor > LLDP** menu path displays the **Neighbours**, **LLDP-MED Neighbours** and **Port Statistics** sub-menus.

The IEEE 802.1ab Link Layer Discovery Protocol (LLDP) standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

Monitor > LLDP > Neighbours

The **Monitor > LLDP > Neighbours** menu path provides a status overview of all LLDP neighbours.

| LLDP Remote Device Summary | | | | | | |
|-------------------------------|------------|---------|------------------|-------------|---------------------|--------------------|
| Local Interface | Chassis ID | Port ID | Port Description | System Name | System Capabilities | Management Address |
| No neighbor information found | | | | | | |

The displayed table contains a row for each port on which an LLDP neighbour is detected. If no neighbors are detected, the message “*No neighbour information found*” displays.

The columns hold the following information:

Local Port

The port on which the LLDP frame was received.

Chassis ID

The **Chassis ID** is the identification of the neighbour's LLDP frames (e.g., *00-C0-F2-00-00-01*).

Port ID

The identification of the neighbour port (e.g., *1001*).

Port Description

The port description advertised by the neighbor unit.

System Name

System Name is the name advertised by the neighbour unit.

System Capabilities

System Capabilities describes the neighbour unit's capabilities. The possible capabilities are:

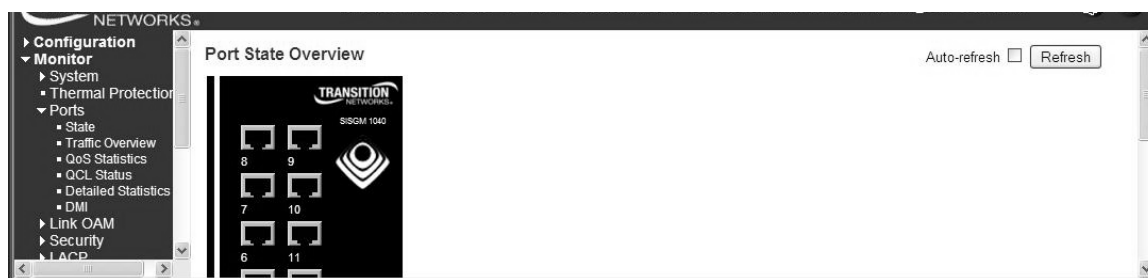
1. **Other**: capabilities other than those listed below.
2. **Repeater**: the neighbour unit functions with repeater capabilities.
3. **Bridge**: the neighbour unit functions with bridge capabilities (e.g., **Bridge(+)** shown above).
4. **WLAN Access Point (WAP)**: the neighbour unit functions with WAP capabilities.
5. **Router**: the neighbour unit functions with router capabilities.
6. **Telephone**: the neighbour unit functions with telephone capabilities.
7. **DOCSIS cable device**: the neighbour unit functions with DOCSIS capabilities.
8. **Station only**: the neighbour unit functions with just station capabilities.
9. **Reserved**: this neighbor unit function description is reserved for future use.

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

Management Address

Management Address is the neighbour unit's address that is used for higher layer entities to assist discovery by the network management. This could for example hold the neighbour's IP address.

When you click the **Management Address** link (e.g., [192.168.1.10 \(IPv4\)](#) in the screen example above), a security dialog opens. Enter the valid password information to display the neighbor's startup screen.



The neighbor device is a Transition Networks Inc. INDURA™ Switch in the example above. You can click the browser Back button to return to the S4224 LLDP Neighbour Information page.

At the INDURA switch, you can also view the Port Statistics from the **Monitor > LLDP** menu path, and click the **Management Address** link to display the INDURA neighbor's startup screen (i.e., go back to the S4224 startup screen display).

Buttons

Refresh: Click to refresh the page immediately.

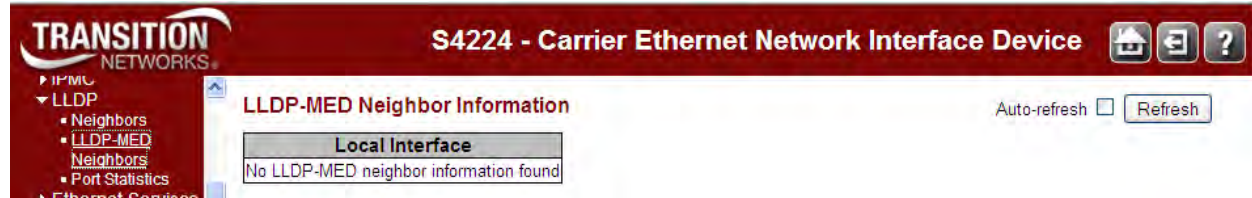
Auto-refresh: Check this box to enable an automatic page refresh every three seconds.

Example

| Local Port | Chassis ID | Remote Port ID | System Name | Port Description | System Capabilities | Management Address |
|------------|-------------------|----------------|-------------|------------------|---------------------|-------------------------------------|
| Port 6 | 00-C0-F2-00-00-01 | 1001 | | Port #1 | Bridge(+) | 192.168.1.10 (IPv4) |

Monitor > LLDP-MED > Neighbours

The **Monitor > LLDP > Neighbours** menu path provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED.



The columns hold the following information:

Port

The port on which the LLDP frame was received.

Device Type

LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

LLDP-MED Network Connectivity Device Definition

LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

1. LAN Switch/Router
2. IEEE 802.1 Bridge
3. IEEE 802.3 Repeater (included for historical reasons)
4. IEEE 802.11 Wireless Access Point
5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

LLDP-MED Endpoint Device Definition

LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.

Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

LLDP-MED Generic Endpoint (Class I)

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other comm related servers, or any device requiring basic services as defined in TIA-1057. Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED Media Endpoint (Class II)

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar. Discovery services defined in this class include media-type-specific network layer policy discovery.

LLDP-MED Communication Endpoint (Class III)

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user. Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, and inventory management).

LLDP-MED Capabilities

LLDP-MED Capabilities describes the neighbor unit's LLDP-MED capabilities. Possible capabilities are:

1. LLDP-MED capabilities
2. Network Policy
3. Location Identification
4. Extended Power via MDI - PSE
5. Extended Power via MDI - PD
6. Inventory
7. Reserved

Application Type

Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are:

1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.
3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.
5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.
6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.

Policy

Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either *Defined* or *Unknown*

Unknown: The network policy for the specified application type is currently unknown.

Defined: The network policy is defined (known).

TAG

TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be *Tagged* or *Untagged*.

Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.

Tagged: The device is using the IEEE 802.1Q tagged frame format.

VLAN ID

VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of **1 - 4094** is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.

Priority

Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (**0 - 7**).

DSCP

DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (**0 - 63**).

Auto-negotiation

Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.

Auto-negotiation status

Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.

Auto-negotiation Capabilities

Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

Buttons

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page.

Messages

Message: "No LLDP-MED neighbor information found" displays at **Monitor > LLDP > LLDP-MED Neighbors**.

Meaning: LLDP-MED is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices; and as such does not apply to links between LAN infrastructure elements.

Recovery: use LLDP-MED devices or ignore the message.

Monitor > LLDP > Port Statistics

The **Monitor > LLDP > Port Statistics** menu path provides an overview of all LLDP traffic.

Two types of LLDP counters are shown. **Global Counters** are counters that refer to the S4224 at the device **level**, while **Local Counters** refer to per port counters for the currently selected S4224.

The screenshot displays the web interface for the S4224 - Carrier Ethernet Network Interface Device. The left sidebar shows a navigation menu with 'Monitor' selected, and 'LLDP' expanded to show 'Port Statistics'. The main content area is titled 'LLDP Global Counters' and includes a 'Global Counters' table with a 'Clear global counters' checkbox (checked) and a timestamp 'Neighbor entries were last changed: 1970-01-01T00:00:00+00:00 (4291 secs. ago)'. Below this is a table for 'LLDP Statistics Local Counters' with columns for Local Interface, Tx Frames, Rx Frames, Rx Errors, Frames Discarded, TLVs Discarded, TLVs Unrecognized, Org. Discarded, Age-Outs, and Clear. The table lists 13 GigabitEthernet interfaces (1/1 to 1/13) with all values set to 0.

| Local Interface | Tx Frames | Rx Frames | Rx Errors | Frames Discarded | TLVs Discarded | TLVs Unrecognized | Org. Discarded | Age-Outs | Clear |
|----------------------|-----------|-----------|-----------|------------------|----------------|-------------------|----------------|----------|-------------------------------------|
| GigabitEthernet 1/1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |
| GigabitEthernet 1/13 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | <input checked="" type="checkbox"/> |

The LLDP Port Statistics page parameters are explained below.

LLDP Global Counters

Clear global counters

If checked the global counters are cleared when the **Clear** button is pressed.

Neighbour entries were last changed on

Shows the date and/or time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

Total Neighbours Entries Added

Shows the number of new entries added since the last S4224 reboot.

Total Neighbours Entries Deleted

Shows the number of new entries deleted since the last S4224 reboot.

Total Neighbours Entries Dropped

Shows the number of LLDP frames dropped due to the entry table being full.

Total Neighbours Entries Aged Out

Shows the number of entries deleted due to Time-To-Live (TTL) expiring.

LLDP Statistics Local Counters

The displayed table contains a row for each port. The columns hold the following information:

Local Interface

The port on which LLDP frames are received or transmitted (e.g., GigabitEthernet 1/1 or 2.5GigabitEthernet 1/2).

Tx Frames

The number of LLDP frames transmitted on the port.

Rx Frames

The number of LLDP frames received on the port.

Rx Errors

The number of received LLDP frames containing some kind of error.

Frames Discarded

If an LLDP frame is received on a port, and the S4224's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out. See IEEE Std 802.1AB for more information.

TLVs Discarded

Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized

The number of well-formed TLVs, but with an unknown type value.

Org. Discarded

The number of organizationally received TLVs.

Age-Outs

Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the **Age-Out** counter is incremented.

Clear

If checked the global counters are cleared when the **Clear** button is pressed.

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clears the **local counters**. If you click the **OK** button at the webpage confirmation dialog, all counters (including **global counters**) are cleared upon reboot.

Auto-refresh: Check this checkbox to automatically refresh the page every three seconds.

Monitor > Ethernet Services

Service Frame (Traffic) Colors - Green / Yellow / Red

The MEF specifies traffic “coloring” as a way to mark traffic as ‘in profile’ or ‘out of profile’ as it leaves the ingress UNI. MEF 10 specifies three levels of Bandwidth Profile compliance:

Green: Service Frame subject to SLA; in-profile and conform to BW profile; delivered per the service performance objectives specified. A service frame is green if it is conformant with the CIR of the bandwidth profile.

Yellow: Service Frame not subject to SLA; out of profile but typically not immediately discarded; not delivered per the service performance objectives; may get discarded by the network. A service frame is yellow if it is not conformant with the EIR of the bandwidth profile.

Red: Service Frame discarded; out of profile and immediately discarded. A service frame is red if it is conformant with neither the CIR nor EIR of the bandwidth profile.

> EVC Statistics

The **Monitor > Ethernet Services > EVC Statistics** menu path provides NNI port traffic statistics for the selected EVC. It also shows counters for UNI ports of ECEs mapping to the EVC.

The screenshot shows the web interface for a Transition Networks S4224 device. The main content area displays 'EVC Statistics' for EVC ID 1. The interface includes a navigation menu on the left with options like Configuration, Monitor, System, Ports, Link OAM, DHCP, Security, LACP, Loop Protection, Spanning Tree, MVR, IPMC, LLDP, and Ethernet Services. The EVC Statistics section has a table with columns for Clear, Port, Green (Frames Rx/Tx, Bytes Rx/Tx), Yellow (Frames Rx/Tx, Bytes Rx/Tx), Red (Frames Rx, Bytes Rx), and Discarded (Frames Rx/Tx, Bytes Rx/Tx). The table shows zero counts for all metrics across all ports (3, 4, 5, 6).

| Clear | Port | Green | | Yellow | | Red | | Discarded | | | | | | | |
|--------------------------|------|--------|----|--------|----|--------|----|-----------|----|----|----|---|---|---|---|
| | | Frames | | Bytes | | Frames | | Bytes | | | | | | | |
| | | Rx | Tx | Rx | Tx | Rx | Rx | Rx | Tx | Rx | Tx | | | | |
| <input type="checkbox"/> | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| <input type="checkbox"/> | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| <input type="checkbox"/> | 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| <input type="checkbox"/> | 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

The EVC Statistics table parameters are explained below.

EVC ID

Enter an existing EVC ID to display its statistics. If the EVC has not been created, the message “EVC ID x is Invalid!” displays.

Clear

This box is used to mark a port for clearance in next Clear operation.

Rx Green

The number of green frames (or bytes) received.

Tx Green

The number of green frames (or bytes) transmitted.

Rx Yellow

The number of yellow frames (or bytes) received.

Tx Yellow

The number of yellow frames (or bytes) transmitted.

Rx Red

The number of red frames (or bytes) received.

Rx Discarded

The number of discarded frames (or bytes) in the ingress queue system.

Tx Discarded

The number of discarded frames (or bytes) in the egress queue system.

Buttons

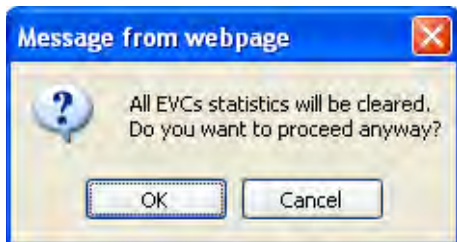
- Frames:** Show frames statistics only.
- Bytes:** Show bytes statistics only.
- Both:** Show both frames and bytes statistics.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for selected ports.

Clear All: Clears the counters for all ports. Displays the message “*All EVCs statistics will be cleared. Do you want to proceed anyway?*”.



Click the **OK** button to clear (zero out) the EVC statistics counters for selected ports, or click the **Cancel** button to clear the webpage message but leave the EVC statistics counters the same.

ECE Statistics

The **Monitor > Ethernet Services > EVC Statistics** menu path provides UNI port traffic statistics for available ECE. It also shows counters for NNI ports of the EVC to which the ECE is mapped.

| Clear | Port | Green | | | | Yellow | | | | Red | | Discarded | | | | |
|--------------------------|------|--------|----|-------|----|--------|----|-------|----|--------|-------|-----------|----|-------|----|---|
| | | Frames | | Bytes | | Frames | | Bytes | | Frames | Bytes | Frames | | Bytes | | |
| | | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Rx | Rx | Tx | Rx | Tx | |
| <input type="checkbox"/> | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| <input type="checkbox"/> | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| <input type="checkbox"/> | 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| <input type="checkbox"/> | 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

The ECE Statistics table parameters are explained below.

Clear

This box is used to mark a port for clearance in next Clear operation.

Port

The UNI/NNI port for the ECE.

Rx Green Frames and Bytes

The number of green bytes and frames received.

Tx Green Frames and Bytes

The number of green bytes and frames transmitted.

Rx Yellow Frames and Bytes

The number of yellow bytes and frames received.

Tx Yellow Frames and Bytes

The number of yellow bytes and frames transmitted.

Rx Red Frames and Bytes

The number of red bytes and frames received.

Rx Discarded Frames and Bytes

The number of bytes and frames discarded in the ingress queue system.

Tx Discarded Frames and Bytes

The number of bytes and frames discarded in the egress queue system.

Buttons

- Frames:** Show frames statistics only.
- Bytes:** Show bytes statistics only.
- Both:** Show both frames and bytes statistics.

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for selected ports.

Clear All: Clears the counters for all ports. Displays the message “*All EVCs statistics will be cleared. Do you want to proceed anyway?*”. Click the **OK** button to clear (zero out) the EVC statistics counters for selected ports, or click the **Cancel** button to clear the webpage message but leave the EVC statistics counters the same.

Monitor > Performance Monitor

The **Monitor > Performance Monitor** menu path displays the performance monitor DM, LM and EVC traffic statistics and measurement Interval information for the selected measurement interval and/or MEP instance. The screen below shows Measurement Interval ID 2 and MEP Instance 1 statistics with no MEP Detailed Info shown.

The screenshot shows the web interface for a Transition Networks device (S4224 - Carrier Ethernet Network Interface Device). The main content area is titled "Performance Monitor Loss Measurement Statistics". It includes a navigation menu on the left with options like Performance, Monitor, LM Statistics, DM Statistics, EVC Statistics, Interval Information, PTP, MAC Table, VLANs, and DDMI. The main area has a title bar with "Auto-refresh" (unchecked), "Refresh", and "Delete All" buttons. Below the title bar, there are checkboxes for "Measurement Interval ID" (set to 2), "MEP Instance" (set to 1), and "MEP Detailed Info." (unchecked). A table displays the statistics, but it is currently empty, showing "No more entries".

| Measurement Interval ID | MEP Instance | Residence Port | Priority | Rate | TX | RX | Near End Loss | | Far End Loss | |
|-------------------------|--------------|----------------|----------|------|----|----|---------------|-------|--------------|-------|
| | | | | | | | Count | Ratio | Count | Ratio |
| No more entries | | | | | | | | | | |

Performance Monitor Loss Measurement Statistics

The **Configuration > Performance Monitor > LM Statistics** parameters are described below.

Measurement Interval ID

The measurement interval for the performance monitor data sets.

MEP Instance

The MEP instance for the performance monitor data sets.

Residence Port

The residence port for the MEP.

Priority

The priority to be inserted as PCP bits in TAG (if any).

Rate

Selected the frame rate of CCM/LMM PDU. This is the inverse of transmission period as described in Y.1731.

TX

The number of frames transmitted.

RX

The number of frames received.

Near End Loss Count

The near end loss count.

Near End Loss Ratio

The near end loss ratio.

Far End Loss Count

The far end loss count.

Far End Loss Ratio

The far end loss ratio.

Domain

Port: This is a MEP in the Port Domain. 'Flow Instance' is a Port.

Evc: This is a MEP in the EVC Domain. 'Flow Instance' is a EVC.

VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN.

Direction

Up: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.

Down: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

Level

The MEG level of this MEP.

Flow Instance

The MEP is related to this flow - See '**Domain**' above.

Tagged VID

Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.

EVC MIP: On Serval, this is the Subscriber VID that identifies the subscriber flow in this EVC where the MIP is active.

MEP ID

This value will become the transmitted two byte CCM MEP ID.

MAC Address

The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Peer MEP ID

This value will become an expected MEP ID in a received CCM - see '**cMEP**'.

Peer MAC Address

This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.

Buttons

Auto-refresh : Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Delete All: Delete all table entries.

|<<: Updates the table entries, starting from the first available entry.

<<: Updates the table entries, ending at the last entry currently displayed.

>>: Updates the table entries, starting from the last entry currently displayed.

>>|: Updates the table entries, ending at the last available entry.

Performance Monitor Delay Measurement Statistics

This page provides the performance monitor loss measurement traffic statistics for the selected measurement interval ID and Delay Measurement instance.

The screenshot shows the web interface for a Transition Networks S4224 device. The main content area is titled "Performance Monitor Delay Measurement Statistics". It includes an "Auto-refresh" checkbox, a "Refresh" button, a "Delete All" button, and navigation buttons for page control. Below these are filters for "Measurement Interval ID" (set to 1), "MEP Instance" (set to All), and radio buttons for "One-way", "Two-way" (selected), and "Both". There is also a checkbox for "MEP Detailed Info.". A table with the following columns is displayed: Measurement Interval ID, MEP Instance, Residence Port, Priority, Rate, Unit, TX, RX, and a sub-section for "Two-way Delay" containing Average, Average Delay Variation, Min., Max., and Bin. The table currently shows "No more entries".

The **Monitor > Performance Monitor > DM Statistics** parameters are described below.

Measurement Interval ID

The measurement interval for the performance monitor data sets.

MEP Instance

The MEP instance for the performance monitor data sets.

Residence Port

The residence port for the MEP.

Priority

The priority to be inserted as PCP bits in TAG (if any).

Rate

The gap between transmitting 1DM/DMM PDU in 10ms. The range is **10** to **65535**.

Unit

The time resolution.

TX

The number of frame transmitted.

RX

The number of frame received.

One-way Far to Near Average Delay

The one-way far to near average delay.

One-way Far to Near Average Delay Variation

The one-way far to near average delay variation.

One-way Far to Near Min. Delay

The minimum one-way near to far delay.

One-way Far to Near Max. Delay

The maximum one-way near to far delay.

One-way Near to Far Average Delay

The number of red received.

One-way Near to Far Average Delay Variation

The one-way near to far average delay variation.

One-way Near to Far Min. Delay.

The minimum one-way near to far delay.

One-way Near to Far Max. Delay.

The maximum one-way near to far delay.

Two-way Delay Average Delay

The two-way average delay.

Two-way Average Delay Variation

The two-way average delay variation.

Two-way Min. Delay

The minimum two-way delay.

Two-way Max. Delay

The maximum two-way delay.

Domain

Port: This is a MEP in the Port Domain. 'Flow Instance' is a Port.

Evc: This is a MEP in the EVC Domain. 'Flow Instance' is a EVC.

VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN.

Direction

Up: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.

Down: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

Level

The MEG level of this MEP.

Flow Instance

The MEP is related to this flow - See 'Domain'.

Tagged VID

Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.

EVC MIP: On Serval, this is the Subscriber VID that identify the subscriber flow in this EVC where the MIP is active.

MEP ID

This value will become the transmitted two byte CCM MEP ID.

MAC Address

The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Peer MEP ID

This value will become an expected MEP ID in a received CCM - see 'cMEP'.

Peer MAC Address

This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.

Bin

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

If the measurement threshold is 5000 us and the total number of Measurement Bins is four, the following example applies:

| Bin | Threshold | Range |
|------|-----------|--|
| bin0 | 0 us | 0 us <= measurement < 5,000 us |
| bin1 | 5,000 us | 5,000 us <= measurement < 10,000 us |
| bin2 | 10,000 us | 10,000 us <= measurement < 15,000 us |
| bin3 | 15,000 us | 15,000 us <= measurement < infinite us |

Buttons

- One-way:** Show one-way statistics only.
- Two-way:** Show two-way statistics only.
- Both:** Show both frames and bytes statistics.

Auto-refresh : Check this box to refresh the page automatically every 3 seconds.

Delete: Click to refresh the page immediately.

Delete All: Delete all table entries.

|<<: Updates the table entries, starting from the first available entry.

<<: Updates the table entries, ending at the last entry currently displayed.

>>: Updates the table entries, starting from the last entry currently displayed.

>>]: Updates the table entries, ending at the last available entry.

Performance Monitor EVC Statistics

This page provides the performance monitor EVC traffic statistics for the selected measurement interval ID and EVC instance.

The screenshot shows the web interface for a Transition Networks device (S4224 - Carrier Ethernet Network Interface Device). The main content area is titled "Performance Monitor EVC Statistics". It features a navigation menu on the left with options like Ethernet Services, Performance Monitor, LM Statistics, DM Statistics, EVC Statistics, Interval Information, PTP, MAC Table, VLANs, and PDM. The main area has a title bar with "S4224 - Carrier Ethernet Network Interface Device" and navigation icons. Below the title bar, there are controls for "Auto-refresh" (checkbox), "Refresh", "Delete All", and navigation buttons (|<<, <<, >>, >>|). There are also input fields for "Measurement Interval ID" (set to 1) and "EVC Instance" (set to All). Radio buttons are present for "Frames" (selected), "Bytes", and "Both". Below these controls is a table with the following structure:

| Measurement Interval ID | EVC Instance | Port | Cos | Green Frames | | Yellow Frames | | Red Frames | Discarded Frames | |
|-------------------------|--------------|------|-----|--------------|----|---------------|----|------------|------------------|----|
| | | | | Rx | Tx | Rx | Tx | Rx | Rx | Tx |
| No more entries | | | | | | | | | | |

Navigate to **Monitor > Performance Monitor > EVC Statistics**. The parameters are described below.

Measurement Interval ID

The measurement interval for the performance monitor data sets.

EVC Instance

The EVC instance for the performance monitor data sets.

MEP Instance

The MEP instance for the performance monitor data sets.

Residence Port

The residence port for the EVC.

Cos

NNI na -- this is the NNI port and counters are not per Cos on this port.

UNI 0-7 -- this is the UNI port and counters are per Cos on this port.

Rx Green Frames

The number of green received.

Tx Green Frames

The number of green transmitted.

Rx Yellow Frames

The number of yellow received.

Tx Yellow Frames

The number of yellow transmitted.

Rx Red Frames

The number of red received.

Rx Discarded Frames

The number of discarded in the ingress queue system.

Tx Discarded Frames

The number of discarded in the egress queue system.

Buttons

- Frames:** Show frames statistics only.
- Bytes:** Show bytes statistics only.
- Both:** Show both frames and bytes statistics.

Auto-refresh : Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Delete All: Delete all table entries.

|<<: Updates the table entries, starting from the first available entry.

<<: Updates the table entries, ending at the last entry currently displayed.

>>: Updates the table entries, starting from the last entry currently displayed.

>>|: Updates the table entries, ending at the last available entry.

Performance Monitor Measurement Interval Information

This page provides the performance monitor measurement interval information.



Navigate to **Monitor > Performance Monitor > Interval Information**. The parameters are described below.

Information Type

The type of info to display for the performance monitor data sets (**LM**, **DM**, **EVC**, or **ECE**).

Measurement Interval ID

The measurement interval for the performance monitor data sets.

Interval Start Time

The interval start time.

Interval End Time

The interval end time.

Elapsed Time

The elapsed time.

Buttons

- Frames:** Show frames statistics only.
- Bytes:** Show bytes statistics only.
- Both:** Show both frames and bytes statistics.

Auto-refresh : Check this box to refresh the page automatically every 3 seconds.

Refresh: Click to refresh the page immediately.

Delete All: Delete all table entries.

<<<: Updates the table entries, starting from the first available entry.

<<: Updates the table entries, ending at the last entry currently displayed.

>>: Updates the table entries, starting from the last entry currently displayed.

>>>: Updates the table entries, ending at the last available entry.

Monitor > PTP

The **Monitor > PTP** menu path displays PTP External Clock Mode and PTP Clock Configuration information. PTP (Precision Time Protocol) is a network protocol for synchronizing the clocks of computer systems.

The screenshot shows the web interface for a Transition Networks S4224 device. The left sidebar contains a navigation menu with 'Monitor' expanded to show 'PTP'. The main content area is titled 'External I/O Configuration' and includes a table with columns for Port, State, Frequency, and Actual Frequency. Below this is an 'External I/O Options' section with an 'Impedance' dropdown set to '50 Ohms'. The 'PTP Clock Configuration' section contains a table with columns for Clock Instance, Device Type, and a Port List (ports 1-28). The table shows various clock instances and their corresponding device types and port lists.

| Port | State | Frequency | Actual Frequency |
|------------------|---------|-----------|------------------|
| IEEE 1588 Input | Enabled | 1 PPS | 0 Hz |
| IEEE 1588 Output | Enabled | 100000 Hz | 100000.000000 Hz |

| Clock Instance | Device Type | Port List | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------------|-------------|-----------|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 0 | Ord-Bound | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | P2pTransp | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | E2eTransp | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | BC-frontend | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

The PTP clock settings are described below.

External I/O Configuration

Port

SMB Port and direction (**Input** or **Output**).

State

The SMB port current state. The following values are possible:

1. The SMB port is current ly **Enabled**.
2. The SMB port is current ly **Disabled**.

Frequency

Displays the configured Clock Frequency. The following values are possible for input: 1 PPS, 8 KHz, 64 KHz, 1.544 MHz, 2.048 MHz, 10 MHz, 19.44 MHz, and 25 MHz. For output the range is 1-250000000 Hz.

Actual Frequency

Displays the measured frequency (e.g., **0 Hz** or "**100000.000000 Hz**" or - if not available or not configured).

External I/O Options

Impedance

Select the impedance termination of the port. The following values are possible:

- 50 Ohms:** 50 Ohms impedance.
- 75 Ohms:** 75 Ohms impedance.
- Hi-Z:** no impedance termination driven, "tri-stated" or "floating".

PTP Clock Configuration

Clock Instance

Indicates the Instance of a particular Clock Instance [0.-3]. Click on the Clock Instance number ([linked](#)) to monitor the Clock details.

Device Type

Indicates the Type of the Clock Instance. The five Device Types are:

Ord-Bound: Clock's Device Type is Ordinary-Boundary Clock.

P2p Transp: Clock's Device Type is Peer to Peer Transparent Clock.


E2e Transp - Clock's Device Type is End to End Transparent Clock.

MastrOnly: Clock's Device Type is Master Only.

SlaveOnly: Clock's Device Type is Slave Only.

BC-frontend: Clock's Device Type is Boundary Clock - front end.

Port List

Shows the ports configured for that Clock Instance with a green check mark ().

Buttons

Refresh: Click to refresh the page immediately.

PTP Clock's Configuration

Click on a linked Clock Instance in the PTP Clock's Configuration section at the **Monitor > PTP** menu path to display a **PTP Clock's Configuration** page. This page lets you view the current PTP clock settings.

PTP Clock's Configuration Auto-refresh [Refresh](#)

Local Clock Current Time

| PTP Time | Clock Adjustment method | Ports Monitor Page |
|---------------------------------------|-------------------------|-------------------------------|
| 1970-01-07T19:08:32+00:00 421,661,056 | Internal Timer | Ports Monitor |

Clock Default Data Set

| ClockId | Device Type | 2 Step Flag | Clock Identity | Dom | Clock Quality | Pri1 | Pri2 | Protocol | One-Way | VLAN Tag Enable | VID | PCP |
|---------|-------------|-------------|-------------------------|-----|---------------------------|------|------|----------|---------|-----------------|-----|-----|
| 0 | Ord-Bound | True | 00:c0:f2:ff:fe:56:19:08 | 0 | Cl:251 Ac:Unknwn Va:65535 | 128 | 128 | Ethernet | False | True | 1 | 0 |

Clock Current Data Set

| stpRm | Offset From Master | Mean Path Delay | Slave Port | Slave State | Holdover(ppb) |
|-------|--------------------|-----------------|------------|-------------|---------------|
| 0 | 0.000.000.000 | 0.000.000.000 | 0 | FREERUN | N.A. |

Clock Parent Data Set

| Parent Port Identity | Port | PStat | Var | ChangeRate | Grand Master Identity | Grand Master Clock Quality | Pri1 | Pri2 |
|-------------------------|------|-------|-----|------------|-------------------------|----------------------------|------|------|
| 00:c0:f2:ff:fe:56:19:08 | 0 | False | 0 | 0 | 00:c0:f2:ff:fe:56:19:08 | Cl:251 Ac:Unknwn Va:65535 | 128 | 128 |

Clock Time Properties Data Set

| UtcOffset | Valid | leap59 | leap61 | Time Trac | Freq Trac | ptp Time Scale | Time Source |
|-----------|-------|--------|--------|-----------|-----------|----------------|-------------|
| 0 | False | False | False | False | False | True | 160 |

Servo Parameters

| Display | P-enable | I-enable | D-enable | 'P' constant | 'I' constant | 'D' constant |
|---------|----------|----------|----------|--------------|--------------|--------------|
| False | True | True | True | 3 | 80 | 40 |

Filter Parameters

| DelayFilter | period | dist |
|-------------|--------|------|
| 6 | 1 | 2 |

Unicast Slave Configuration

| Index | Duration | IP_Address | Grant | CommState |
|-------|----------|------------|-------|-----------|
| 0 | 100 | 0.0.0.0 | 0 | IDLE |
| 1 | 100 | 0.0.0.0 | 0 | IDLE |
| 2 | 100 | 0.0.0.0 | 0 | IDLE |
| 3 | 100 | 0.0.0.0 | 0 | IDLE |
| 4 | 100 | 0.0.0.0 | 0 | IDLE |

The PTP clock settings are described below.

Local Clock Current time

Shows the local clock data.

PTP Time

Shows the actual PTP time with nanosecond resolution.

Clock Adjustment Method

Shows the actual clock adjustment method. The method depends on the available hardware.

Ports Monitor Page

Click to monitor the port data set for the ports assigned to this clock instance.

Clock Default Dataset

The clock default data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members defined at clock creation time, the dynamic members defined by the system, and configurable members which can be set here.

ClockId

An internal instance id (0-3).

Device Type

Indicates the Type of the Clock Instance. There are five Device Types.

Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock.

P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock.

E2e Transp - Clock's Device Type is End to End Transparent Clock.

Master Only - Clock's Device Type is Master Only.

Slave Only - Clock's Device Type is Slave Only.

BC-frontend: Clock's Device Type is Boundary Clock - front end.

2 Step Flag

Static member: defined by the system, true if two-step Sync events and Pdelay_Resp events are used.

Ports

The total number of physical ports in the node.

Clock Identity

It shows unique clock identifier.

Dom

Clock domain (0-127).

Clock Quality

The clock quality is determined by the system, and holds 3 parts: Clock Class, Clock Accuracy and OffsetScaledLog Variance as defined in IEEE1588.

The Clock Accuracy values are defined in IEEE1588 table 6 (currently the clock Accuracy is set to 'Unknown' as default).

Pri1

Clock priority 1 (0 - 255) used by the BMC master select algorithm.

Pri2

Clock priority 2 (0 - 255) used by the BMC master select algorithm.

Protocol

Transport protocol used by the PTP protocol engine, either:

Ethernet PTP over Ethernet multicast

ip4multi PTP over IPv4 multicast

ip4uni PTP over IPv4 unicast

Note : IPv4 unicast protocol only works in Master only and Slave only clocks . See the Device Type parameter.

In a unicast Slave only clock you also must configure which master clocks to request Announce and Sync messages from. See 'Unicast Slave Configuration'.

One-Way

If **True**, one-way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.

VLAN Tag Enable

Enables the VLAN tagging for the PTP frames. **Note:** Packets are only tagged if the port is configured for vlan tagging (i.e., Port Type != Unaware and PortVLAN mode == None, and the port is member of the VLAN).

VID

VLAN Identifier used for tagging the PTP frames.

PCP

Priority Code Point value used for PTP frames.

Clock current Data Set

The clock current data set is defined in the IEEE 1588 Standard. The current data set is dynamic

stpRm

Steps Removed : It is the number of PTP clocks traversed from the grandmaster to the local slave clock.

Offset from master

Time difference between the master clock and the local slave clock, measured in ns (e.g., 0.000,000,000).

mean Path Delay

The mean propagation time for the link between the master and the local slave (e.g., 0.000,000,000).

Slave Port

Shows which port is in slave mode. The value is **0** if no ports are in slave mode.

Slave State

Shows synchronization state of the slave. (e.g., FREERUN, etc.).

Holdover(ppb)

After the slave has been in Locked mode during the stabilization period, this value shows the actual clock offset between the freerun and the actual holdover frequency, the value is shown in parts per billion (ppb). During the stabilization period, the value is shown as **N.A.** The default stabilization period is **60** seconds; it can be changed from the CLI interface.

Clock Parent Data Set

The clock parent data set is defined in the IEEE 1588 standard. The parent data set is dynamic.

Parent Port Identity

Clock identity for the parent clock, if the local clock is not a slave, the value is the clock's own id.

Port

Port Id for the parent master port.

PStat

Parents Stats (always **False**).

Var

It is observed parent offset scaled log variance.

Change Rate

Observed Parent Clock Phase Change Rate (i.e., the slave clocks rate offset compared to the master) (unit = ns per second).

Grand Master Identity

Clock identity for the grand master clock, if the local clock is not a slave, the value is the clocks own id.

Grand Master Clock Quality

The clock quality announced by the grand master. (See description of Clock Default DataSet:Clock Quality.)

Pri1

Clock priority 1 announced by the grand master.

Pri2

Clock priority 2 announced by the grand master.

Clock Time Properties Data Set

The clock time properties data set is defined in the IEEE 1588 Standard. The data set is both configurable and dynamic, i.e. the parameters can be configured for a grandmaster. In a slave clock the parameters are overwritten by the grandmasters timing properties. The parameters are not used in the current PTP implementation.

The valid values for the Time Source parameter are:

- 16** (0x10) ATOMIC_CLOCK
- 32** (0x20) GPS
- 48** (0x30) TERRESTRIAL_RADIO
- 64** (0x40) PTP
- 80** (0x50) NTP
- 96** (0x60) HAND_SET
- 144** (0x90) OTHER
- 160** (0xA0) INTERNAL_OSCILLATOR

Servo Parameters

The default clock servo uses a PID regulator to calculate the current clock rate. The formula is:
clockAdjustment =

$$\begin{aligned} & \text{OffsetFromMaster} / \text{P constant} \\ & + \text{Integral}(\text{OffsetFromMaster}) / \text{I constant} \\ & + \text{Differential}(\text{OffsetFromMaster}) / \text{D constant} \end{aligned}$$

Display

If true then Offset From Master, MeanPathDelay and clockAdjustment are logged on the debug terminal.

P-enable

If true the **P** part of the algorithm is included.

I-Enable

If true the **I** part of the algorithm is included.

D-enable

If true the **D** part of the algorithm is included.

'P' constant

[1..1000] see above.

'I' constant

[1..10000] see above.

'D' constant

[1..10000] see above.

Filter Parameters

The default delay filter is a low pass filter, with a time constant of $2 * \text{DelayFilter} * \text{DelayRequestRate}$.

The default offset filter uses a minimum offset or a mean filter method.

The minimum measured offset during **Period** samples is used in the calculation.

The distance between two calculations is **Dist** periods.

If **Dist** is 1 the offset is averaged over the **Period**,

If **Dist** is >1 the offset is calculated using 'min' offset.

DelayFilter

See above

Period

See above

dist

See above

Unicast Slave Configuration

When operating in IPv4 Unicast mode, the slave is configured with up to five master IP addresses. The slave then requests Announce messages from all the configured masters. The slave uses the BMC algorithm to select one as master clock, the slave then request Sync messages from the selected master.

Duration

The number of seconds a master is requested to send Announce/Sync messages. The request is repeated from the slave each Duration/4 seconds.

IP_address

IPv4 Address of the master clock.

grant

The granted repetition period for the sync message

CommState

The state of the communication with the master, possible values are:

IDLE : The entry is not in use.

INIT : Announce is sent to the master (Waiting for a response).

CONN : The master has responded.

SELL : The assigned master is selected as current master.

SYNC : The master is sending Sync messages.

Buttons

Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

PTP Clock's Port Data Set Configuration

Click on the [Ports Monitor Page](#) link in the PTP Clock's Configuration section to display the **PTP Clock's Port Data Set Configuration** table. The port data set is defined in the IEEE 1588 Standard.

The port data set is defined in the IEEE 1588 Standard. It holds three groups of data: the static members, the dynamic members, and configurable members which can be set here.

| PTP Clock's Port Data Set Configuration | | | | | | | | | | | | |
|---|------|-----|-----------------|-----|-----|-----|-----|-----|-----------------|-----------------|----------------|---------|
| Port | Stat | MDR | PeerMeanPathDel | Anv | ATo | Syv | Dlm | MPR | Delay Asymmetry | Ingress Latency | Egress Latency | Version |
| 2 | dsbl | 0 | 0.000,000,000 | 1 | 3 | 0 | e2e | 3 | 0.000,000,000 | 0.000,000,000 | 0.000,000,000 | 2 |
| 3 | dsbl | 0 | 0.000,000,000 | 1 | 3 | 0 | e2e | 3 | 0.000,000,000 | 0.000,000,000 | 0.000,000,000 | 2 |
| 4 | dsbl | 0 | 0.000,000,000 | 1 | 3 | 0 | e2e | 3 | 0.000,000,000 | 0.000,000,000 | 0.000,000,000 | 2 |

The related **The PTP Clock's Port Data Set Configuration** table parameters are explained below.

Port

Port number (1 - the max number of ports).

Stat

Dynamic member portState: Current state of the port.

MDR

Dynamic member log Min Delay Req Interval: The delay request interval announced by the master.

Peer Mean Path Del

The path delay measured by the port in P2P mode. In E2E mode this value is **0**.

Anv

The interval for issuing announce messages in master state. The valid range is -3 to 4.

ATo

The timeout for receiving announce messages on the port. The valid range is 1 to 10.

Syv

The interval for issuing sync messages in master. The valid range is -7 to 4.

Dlm

Configurable member delayMechanism; the delay mechanism used for the port:

e2e : End to end delay measurement

p2p : Peer to peer delay measurement.

Can be defined per port in an Ordinary/Boundary clock. In a transparent clock all ports use the same delay mechanism, determined by the clock type.

MPR

The interval for issuing Delay_Req messages for the port in E2e mode. This value is announced from the master to the slave in an announce message. The value is reflected in the MDR field in the Slave. The interval for issuing Pdelay_Req messages for the port in P2P mode

Note: The interpretation of this parameter has changed from v 1.2 to v 2.0. In earlier versions the value was interpreted relative to the Sync interval; this was a violation of the standard, so now the value is interpreted as an interval. I.e. $MPR = 0 \Rightarrow 1$ Delay_Req pr sec, independent of the Sync rate. The valid range is -7 to 5.

Delay Asymmetry

The transmission delay asymmetry for a link. See IEEE 1588 Section 7.4.2 Communication path asymmetry.

If the transmission delay for a link is not symmetric, the asymmetry can be configured here, see IEEE 1588 Section 7.4.2 Communication path asymmetry. The valid range is -100000 to 100000.

Ingress latency

Ingress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2.
The valid range is -100000 to 100000.

Egress Latency

Egress latency measured in ns, as defined in IEEE 1588 Section 7.3.4.2.
The valid range is -100000 to 100000.

Version

The current implementation only supports PTP version 2.

Buttons

Auto-refresh : Check this box to refresh the page automatically every three seconds.

Refresh: Click to refresh the page immediately.

Monitor > MAC Table

The **Monitor > MAC Table** menu path displays the entries in the MAC Table. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Switching of frames is based on the DMAC address contained in the frame. The S4224 builds a table that maps MAC addresses to S4224 ports for knowing which ports the frames should go to (based on the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and S4224 ports.

The frames also contain a MAC address (SMAC address) which shows the MAC address of the equipment sending the frame. The SMAC address is used by the S4224 to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.

The screenshot shows the 'MAC Address Table' in the S4224 web interface. The table has the following structure:

| Type | VLAN | MAC Address | Port Members | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------|------|-------------------|--------------|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-----|
| | | | CPU 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | MGM |
| Dynamic | 1 | 00-1B-11-B2-6D-4B | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Static | 1 | 00-C0-F2-56-16-D1 | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Static | 1 | 01-00-0C-CC-CC-CC | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Static | 1 | 01-80-C2-00-00-30 | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Static | 1 | 01-80-C2-00-00-38 | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Static | 1 | 33-33-00-00-00-01 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Static | 1 | 33-33-00-00-00-02 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Static | 1 | 33-33-FF-56-16-D0 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Static | 1 | FF-FF-FF-FF-FF-FF | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "Start from VLAN" and "and MAC address" input fields let you select the starting point in the MAC Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

Click the >> button to use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached, the text "No more entries" displays in the table. Use the |<< button to start over.

The MAC Address Table columns are explained below.

Type

Indicates whether the entry is a **Static** or a **Dynamic** entry.

VLAN

The VLAN ID of the entry.

MAC Address

The MAC address of the entry in the format 00-00-00-00-00-00.

Port Members

A green check mark (✓) indicates if a port is a member of the entry (CPU, ports 1-6).

Buttons

Auto-refresh: Check this checkbox to automatically refresh the page every three seconds. .

Refresh: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

Clear: Flushes all dynamic entries.

|<<: Updates the table starting from the first entry in the MAC Table (i.e., the entry with the lowest VLAN ID and MAC address).

>>: Updates the table, starting with the entry after the last entry currently displayed.

Monitor > VLANs

The **Monitor > VLANs** menu path displays the **VLAN Membership** and **VLAN Ports** sub-menus.

The S4224 will be compliant with IEEE 802.1Q standard. The S4224 is capable of VLAN bridging and filtering. By default the devices comes up with all ports belonging to the same VLAN.

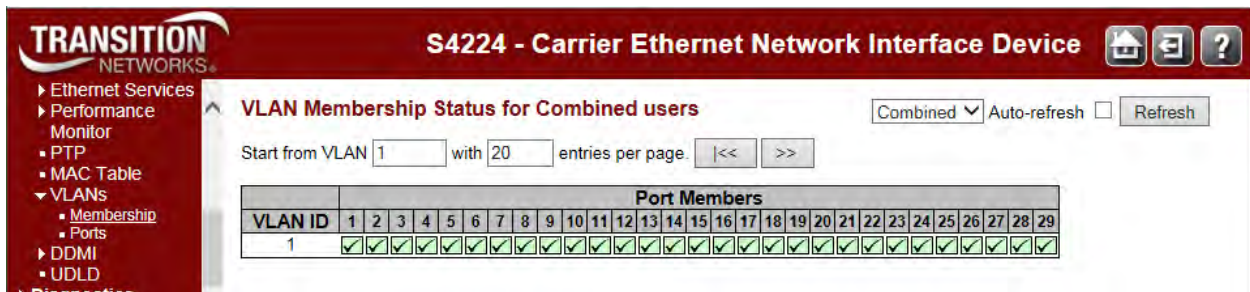
The S4224 supports the entire range of 4k VLAN IDs except for the following:

- a. VLAN ID = 0 is used for priority tagged traffic and will not be used.
- b. VLAN ID = 1 is used for the S4224 default VLAN (native VLAN ID).
- c. VLAN ID = 4094 is reserved and not available for normal traffic.

Each VLAN has a unique string for identification called the "VLAN Name", no spaces will be allowed. A Maximum of 64 VLANs can have VLAN names and the name is restricted to 32 bytes. Only alphabets and digits are allowed as valid characters with at least one alphabet to be part of the name.

Monitor > VLANs > VLAN Membership

The **Monitor > VLANs > VLAN Membership** menu path provides an overview of membership status of VLAN users. The default VLAN Membership Status page is shown below (for the 'Combined' selection).



Each page shows up to 99 entries from the VLAN table (default being 20), selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input field allows the user to select the starting point in the VLAN Table.

Clicking the **Refresh** button will update the displayed table starting from that or the closest next VLAN Table match.

The >> button will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached, the text "No data exists for the selected user" is shown in the table. Use the <<< button to start over.

Clicking a Port Members checkbox alternately displays "VLAN included", then "VLAN not included" and then "Forbidden port" in the cursor over help (CoH).

The **VLAN Membership** parameters are explained below.

VLAN USER

Various internal software modules may use VLAN services to configure VLAN memberships on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

Combined: Displays a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

Admin: Various internal software modules may use VLAN services to configure VLAN memberships on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.



NAS: NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server.

GVRP: GARP VLAN Registration Protocol lets network devices share VLAN information and use the information to modify existing VLANs or create new VLANs, automatically.

MVR: MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.


MEP: displays the status for all SOAM Maintenance End Point) user types.


EVC: displays the status for all EVC (Ethernet Virtual Circuit) user types.


RMirror: displays the status for remote mirror VLAN user types.

Port Members


A row of check boxes for each port is displayed for each VLAN ID.

If a port is included in a VLAN, the following image displays: .

If a port is in the forbidden port list, the following image displays: .

If a port is in the forbidden port list and at the same time attempted inclusion in the VLAN, the following image displays: . The port will not be a member of the VLAN in this case.

Buttons

Combined : Select VLAN Users from this drop down list (Combined, Admin, or Various internal software modules as described above).

Auto-refresh: Check this box to automatically refresh the page every three seconds.

Refresh: Click to refresh the page immediately.

Monitor > VLANs > Ports

The **Monitor > VLANs > Ports** menu path provides VLAN Port Status.

The S4224 ports can be configured with a default or native VLAN id, so that all untagged and priority tagged traffic will be classified to this VLAN ID. The native VLAN ID for all ports is set to 1 but is configurable on a per-port basis. Hence all ports by default belong to the same broadcast domain.

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

VLAN Port Status for Combined users

Combined Auto-refresh Refresh

| Port | Port Type | Ingress Filtering | Frame Type | Port VLAN ID | Tx Tag | Untagged VLAN ID | Conflicts |
|------|-----------|-------------------------------------|------------|--------------|-----------|------------------|-----------|
| 1 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 2 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 3 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 4 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 5 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 6 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 7 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 8 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 9 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 10 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 11 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 12 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 13 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 14 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |
| 15 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag All | | No |

The VLAN User module uses the services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID or UVID.

VLAN User

Various internal software modules may use VLAN services to configure VLAN port configuration on the fly. The VLAN user type drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. If a given software modules hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table.

Combined: The "Combined" entry shows a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

Admin: Various internal software modules may use VLAN services to configure VLAN port configuration on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules.

If a given software modules hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table.

NAS: Displays only the NAS VLAN users' membership status.

GVRP: GARP VLAN Registration Protocol lets network devices share VLAN information and use the information to modify existing VLANs or create new VLANs, automatically.

MVR: Displays only the MVR VLAN users' membership status.

MSTP: Displays only the MSTP VLAN users' membership status.

ERPS: Displays only the ERPS VLAN users' membership status.

MEP: Displays only the MEP VLAN users' membership status.

EVC: Displays only the EVC VLAN users' membership status.

- Combined
- Admin
- NAS
- GVRP
- MVR
- MSTP
- ERPS
- MEP
- EVC
- VCL
- RMirror

VCL: Displays only the VCL VLAN users' membership status.

RMirror: Displays only the VCL remote mirror users' membership status.

Port

The logical port for the settings contained in the same row.

Port Type

Shows the port type (Unaware, C-Port, S-Port, or S-Custom-Port) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.

Unaware: all frames are classified to the Port VLAN ID and tags are not removed.

C-port: a Customer Port.

S-port: a Service port.

Custom S-port: an S-port with Custom TPID.

Ingress Filtering

Shows whether a given user wants ingress filtering enabled or not. The field is empty if not overridden by the selected user.

Frame Type

Shows the acceptable frame types (All, Taged, Untagged) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.

Port VLAN ID

Shows the Port VLAN ID (PVID) that a given user wants the port to have. The field is empty if not overridden by the selected user.

Tx Tag

Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port. The field is empty if not overridden by the selected user.

Untagged VLAN ID

If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field will show the VLAN ID the user wants to tag or untag on egress.

The field is empty if not overridden by the selected user.

Conflicts

Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress.

Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority.

If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module.

The "Combined" user reflects what is actually configured in hardware.

Buttons

Auto-refresh: Check this box to automatically refresh the page every three seconds.

Refresh: Click to refresh the page immediately.

Examples

An example of the VLAN Port Status for “**Combined**” users is shown below.

| VLAN Port Status for Combined users | | | | | | | |
|---|-----------|-------------------------------------|------------|--------------|------------|------------------|-----------|
| Combined <input type="button" value="Auto-refresh"/> <input type="button" value="Refresh"/> | | | | | | | |
| Port | Port Type | Ingress Filtering | Frame Type | Port VLAN ID | Tx Tag | Untagged VLAN ID | Conflicts |
| 1 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Tag UVID | 10 | No |
| 2 | C-Port | <input checked="" type="checkbox"/> | All | 2 | Tag UVID | 20 | No |
| 3 | C-Port | <input checked="" type="checkbox"/> | All | 3 | Untag All | | No |
| 4 | C-Port | <input checked="" type="checkbox"/> | Tagged | 1 | Tag All | | No |
| 5 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag PVID | | No |
| 6 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag PVID | | No |
| 7 | C-Port | <input checked="" type="checkbox"/> | All | 1 | Untag PVID | | No |

VLAN Port Status for “**MVR**” user is shown below.

| VLAN Port Status for MVR user | | | | | | | |
|--|-----------|-------------------|------------|--------------|-----------|------------------|-----------|
| MVR <input type="button" value="Auto-refresh"/> <input type="button" value="Refresh"/> | | | | | | | |
| Port | Port Type | Ingress Filtering | Frame Type | Port VLAN ID | Tx Tag | Untagged VLAN ID | Conflicts |
| 1 | C-Port | | All | | Tag UVID | 10 | No |
| 2 | C-Port | | All | | Tag UVID | 20 | No |
| 3 | C-Port | | All | | Untag All | | No |

ERPS:

| VLAN Port Status for ERPS user | | | | | | | |
|---|-----------|-------------------------------------|------------|--------------|--------|------------------|-----------|
| ERPS <input type="button" value="Auto-refresh"/> <input type="button" value="Refresh"/> | | | | | | | |
| Port | Port Type | Ingress Filtering | Frame Type | Port VLAN ID | Tx Tag | Untagged VLAN ID | Conflicts |
| 1 | | <input checked="" type="checkbox"/> | | | | | No |
| 2 | | <input checked="" type="checkbox"/> | | | | | No |
| 3 | | <input checked="" type="checkbox"/> | | | | | No |
| 4 | | <input checked="" type="checkbox"/> | | | | | No |

EVC:

| VLAN Port Status for EVC user | | | | | | | |
|--|-----------|-------------------|------------|--------------|--------|------------------|-----------|
| EVC <input type="button" value="Auto-refresh"/> <input type="button" value="Refresh"/> | | | | | | | |
| Port | Port Type | Ingress Filtering | Frame Type | Port VLAN ID | Tx Tag | Untagged VLAN ID | Conflicts |
| <i>No data exists for the selected user</i> | | | | | | | |

Monitor > DDMI

The **Monitor > DDMI** menu path lets you display DDMI overview and detailed information.

DDMI > Overview

| Port | Vendor | Part Number | Serial Number | Revision | Date Code | Transceiver |
|------|------------|--------------|---------------|----------|------------|-------------|
| 1 | Transition | TN-SFP-SXD | 8672105 | 0000 | 2009-10-27 | 1000BASE_SX |
| 2 | - | - | - | - | - | - |
| 3 | Transition | TN-10GSFP-SR | 102201102 | 0001 | 2010-05-27 | 10G |
| 4 | - | - | - | - | - | - |
| 5 | - | - | - | - | - | - |
| 6 | - | - | - | - | - | - |
| 7 | - | - | - | - | - | - |
| 8 | - | - | - | - | - | - |
| 9 | - | - | - | - | - | - |
| 10 | - | - | - | - | - | - |
| 11 | - | - | - | - | - | - |

Port

The DDMI port number.

Vendor

Indicates the SFP Vendor's name (e.g., Transition).

Part Number

Indicates Vendor Part number (PN) provided by the SFP vendor (TN-10GSFP-SR).

Serial Number

Indicates Vendor Serial number (SN) provided by the SFP vendor (e.g., 8672105).

Revision

Indicates Vendor rev Revision level for part number provided by the SFP vendor.

Data Code

Indicates Date code Vendor's manufacturing date code (e.g., 2010-05-27).

Transceiver

Indicates the Transceiver compatibility (e.g., 1000BASE_SX or 10G).

Click the linked Port number in the DDMI Overview table to display the SFP detailed data as shown and described below.

DDMI > Detailed

This page displays detailed SFP data for a selected port.

The screenshot shows the web interface for a Transition Networks S4224 Carrier Ethernet Network Interface Device. The page title is "S4224 - Carrier Ethernet Network Interface Device". On the left is a navigation menu with options like Configuration, Monitor, System, Ports, Link OAM, DHCP, Security, LACP, Loop Protection, Spanning Tree, MVR, IPMC, LLDP, Ethernet Services, PTP, MAC Table, VLANs, DDMI (Overview, Detailed), UDLD, Diagnostics, and Maintenance. The main content area is titled "Transceiver Information" and "DDMI Information".

Transceiver Information

| | |
|---------------|--------------|
| Vendor | Transition |
| Part Number | TN-10GSFP-SR |
| Serial Number | 102201102 |
| Revision | 0001 |
| Date Code | 2010-05-27 |
| Transceiver | 10G |

DDMI Information

| Type | Current | High Alarm Threshold | High Warn Threshold | Low Warn Threshold | Low Alarm Threshold |
|----------------|-----------|----------------------|---------------------|--------------------|---------------------|
| Temperature(C) | 31.156 | 90.000 | 85.000 | 0.000 | -5.000 |
| Voltage(V) | 3.2840 | 3.6000 | 3.5000 | 3.1000 | 3.0000 |
| Tx Bias(mA) | 6.128 | 20.000 | 15.000 | 2.000 | 1.000 |
| Tx Power(mW) | 0.5888 | 1.0000 | 0.7943 | 0.1862 | 0.1479 |
| Rx Power(mW) | 0.0190 -- | 1.0000 | 0.7943 | 0.1023 | 0.0646 |
| Tx Power(dBm) | -2.30 | 0.00 | -1.00 | -7.30 | -8.30 |
| Rx Power(dBm) | -17.21 | 0.00 | -1.00 | -9.90 | -11.90 |

Transceiver Information

Vendor

Indicates the SFP Vendor's name (e.g., *Transition*).

Part Number

Indicates Vendor Part number (PN) provided by the SFP vendor (*TN-SFP-SXD*).

Serial Number

Indicates Vendor Serial number (SN) provided by the SFP vendor e.g., *102201102*).

Revision

Indicates Vendor rev Revision level for part number provided by the SFP vendor.

Data Code

Indicates Date code Vendor's manufacturing date code (e.g., *2009-10-27*).

Transeiver

Indicates the Transceiver compatibility (e.g., *1000BASE_X*).

DDMI Information

Current

The current value of temperature, voltage, TX bias, TX power, and RX power.

High Alarm Threshold

The high alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.

High Warn Threshold

The high warn threshold value of temperature, voltage, TX bias, TX power, and RX power.

Low Warn Threshold

The low warn threshold value of temperature, voltage, TX bias, TX power, and RX power.

Low Alarm Threshold

The low alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically every 3 seconds.

DDMI Measurement Details

| Type | Unit of Measure | Typical Measurement |
|----------------|---------------------|---------------------|
| Temperature(C) | Degrees (°) Celsius | 51.281 |
| Voltage(V) | Volts | 3.2616 |
| Tx Bias(mA) | milleAmps | 5.024 |
| Tx Power(mW) | milleWatts | 0.2504 |
| Rx Power(mW) | milleWatts | 0.0003 -- |
| Tx Power(dBm) | Decibel-milliwatts | -6.01 |
| Rx Power(dBm) | Decibel-milliwatts | -35.23 |

Note: DDMI information may also be displayed at the **Monitor > Log** menu path as shown below:

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

System Log Information

Auto-refresh Refresh Clear |<< << >> >>|

Level: All
Clear Level: All

The total number of entries is 13 for the given level.

Start from ID 1 with 20 entries per page.

| ID | Level | Time | Message |
|----|---------------|---------------------------|---|
| 1 | Informational | 1970-01-01T00:00:09+00:00 | SYS-BOOTING: Switch just made a cool boot. |
| 2 | Informational | 1970-01-01T00:00:10+00:00 | SyncE selector state change: Free Run |
| 3 | Informational | 1970-01-01T00:00:10+00:00 | DDMI-MODULE_INSERT_REMOVE: Inserted SFP module on Interface 10GigabitEthernet 1/1 |
| 4 | Notice | 1970-01-01T00:00:11+00:00 | LINK-UPDOWN: Interface Vlan 1, changed state to down. |
| 5 | Informational | 1970-01-01T00:00:14+00:00 | DDMI-TEMPERATURE_CHANGED: DoM temperature changed to REGULAR on Interface 10GigabitEthernet ... |
| 6 | Informational | 1970-01-01T00:00:14+00:00 | DDMI-VOLTAGE_CHANGED: DoM voltage changed to REGULAR on Interface 10GigabitEthernet 1/1 |
| 7 | Informational | 1970-01-01T00:00:14+00:00 | DDMI-BIAS_CHANGED: DoM Bias changed to REGULAR on Interface 10GigabitEthernet 1/1 |
| 8 | Informational | 1970-01-01T00:00:14+00:00 | DDMI-BIAS_CHANGED: DoM Tx Power changed to REGULAR on |
| 9 | Informational | 1970-01-01T00:00:14+00:00 | DDMI-BIAS_CHANGED: DoM Rx Power changed to LO ALARM on Interface 10GigabitEthernet 1/1 |

Monitor > UDLD

The **Monitor > UDLD** menu path lets you displays the UDLD status of the ports and neighbor.

The screenshot shows the web interface for a Transition Networks S4224 device. The left sidebar contains a navigation menu with categories like Security, LACP, Loop Protection, Spanning Tree, MVR, IPMC, LLDP, Ethernet Services, PTP, MAC Table, VLANs, DDMI, UDLD, Diagnostics, and Maintenance. The main content area is titled 'S4224 - Carrier Ethernet Network Interface Device' and displays 'Detailed UDLD Status for Port 2'. It includes a dropdown menu for 'Port2', an 'Auto-refresh' checkbox, and a 'Refresh' button. The UDLD status table shows: UDLD Admin state: Enable; Device ID(local): 00-C0-F2-56-16-D0; Device Name(local): -; Bidirectional State: Indeterminant. Below this is the 'Neighbour Status' table, which is currently empty with the message 'No Neighbour ports enabled or no existing partners'.

Detailed UDLD Status for Port x

UDLD Admin State

The current port state of the logical port, **Enable** if any state (Normal, Aggressive) is Enabled.

Device ID(local)

The ID of the local device (e.g., **00-C0-F2-56-1A-90**).

Device Name(local)

The Name of the local device.

Bidirectional State

The current state of the port (e.g., **Indeterminant**).

Neighbour Status

Displays “*No Neighbour ports enabled or no existing partners*” if no status is available.

Port

The current port of neighbour device.

Device ID

The current ID of neighbour device.

Link Status

The current link status of neighbour port.

Device Name

Name of the Neighbour Device.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to enable an automatic refresh of the page at regular intervals.

Diagnostics Main Menu

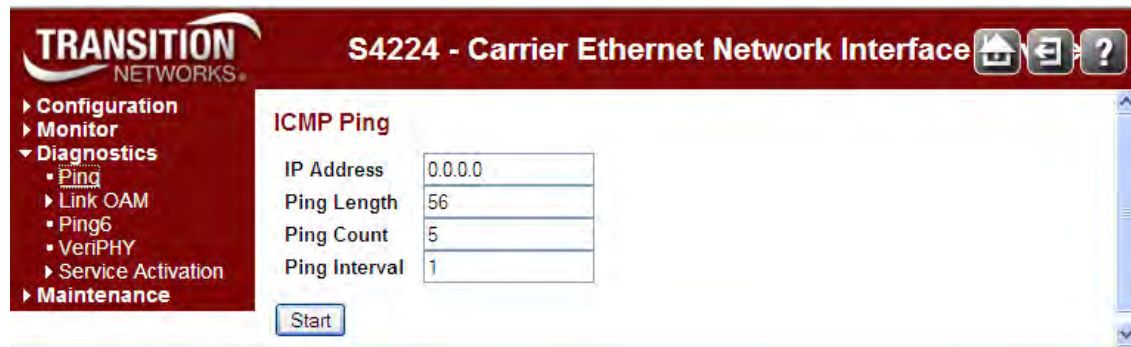
The **Diagnostics** main menu lets you select the **Ping**, **Link OAM**, **Ping6**, **VeriPHY**, and **Service Activation** sub-menus.

Each of these sub-menus is detailed below.



Diagnostics > Ping

This page lets you issue ICMP PING packets to troubleshoot IPv4 connectivity issues.



Ping Procedure

1. Navigate to the **Diagnostics > Ping** menu path.
2. At **IP Address** enter a valid IPv4 address (e.g., 192.168.1.30).
3. At **Ping Length** enter the packet size in bytes.
4. At **Ping Count** enter the number of packets to be sent. The default is 5 pings.
5. At **Ping Interval** enter the interval to be inserted between pings. The default is 1 msec.
6. Click on the **Start** button to retrieve the Ping output.

After you press the **Start** button, five ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

A successful ICMP Ping Output is shown below:



A failed ICMP Ping Output is shown below:

```
ICMP Ping Output
PING server 0.0.0.0, 56 bytes of data:
sendto: No route to host
sendto: No route to host
sendto: No route to host
sendto: No route to host
sendto: No route to host
Sent 0 packets, received 0 OK, 0 bad
```

Click the **New Ping** button to issue another ping. For example:

```
PING6 server ::10.10.132.20
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

A failed Ping is shown below.

```
ICMP Ping Output
PING server 192.168.1.10
recvfrom: Operation timed out
recvfrom: Operation timed out
recvfrom: Operation timed out
recvfrom: Operation timed out
recvfrom: Operation timed out
Sent 5 packets, received 0 OK, 0 bad
```

Diagnostics > Link OAM > MIB Retrieval

The **Diagnostics > Link OAM > MIB Retrieval** menu path lets you retrieve the Local or Remote OAM MIB variable data on a particular port.

The screenshot shows the web interface for the S4224 - Carrier Ethernet Network Interface. The page title is "Link OAM MIB Retrieval". On the left, there is a navigation menu with the following items: Configuration, Monitor, Diagnostics (expanded), Ping, Link OAM (expanded), MIB Retrieval (selected), Ping6, VeriPHY, and Service Activation. The main content area has three radio buttons: "Local" (selected), "Peer", and "Port" (with an adjacent text input field). A "Start" button is located below the radio buttons.

Procedure

1. Make sure the MIB Retrieval Support checkbox is checked at **Configuration > Link OAM > Port Settings**.
2. Navigate to the **Diagnostics > Link OAM > Mib Retrieve** menu path.
3. Select the appropriate radio button to retrieve the content of interest ("Local" or "Peer").
4. Enter the S4224 Port number. This port must be configured and enabled.
5. Click the **Start** button to retrieve the MIB content. A typical display is shown below

The screenshot shows the "Link OAM MIB Retrieval Output" page. It displays the following data:

```

Branch:7
Leaf:aOAMID
Data: 00-00-00-04-

Branch:7
Leaf:aOAMLocalConfiguration
Data: 18-

Branch:7
Leaf:aOAMLocalPDUConfiguration
Data: 00-00-05-dc-

Branch:7
Leaf:aOAMLocalRevision
Data: 00-00-00-00-

Branch:7
Leaf:aOAMLocalState
Data: 00-

```

At the bottom of the page, there is a "New Retrieval" button.

If the Link OAM Mib Retrieve fails, the message "*OAM Error - Invalid request on this port*" displays. Click the browser's Back button to clear the message, verify your selections, and then try the operation again.

Note that the **Monitor > Link OAM > Port Status** page provides detailed Link OAM status.

Diagnostics > Ping6

This page lets you issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

Ping 6 Procedure

1. Navigate to the **Diagnostics > Ping6** menu path.
2. At **IP Address**, enter a valid IPv6 address. This is the destination IP Address for the ping.
3. Enter a **Ping Length** (8 - 1400 bytes). This is the payload size of the ICMP packet. The valid values are **8** to **1400** bytes. The default is **56** bytes.
4. At **Ping Count** enter the number of packets to be sent. This is the count of the ICMP packet. The valid values are **1** to **60** pings. The default is **5** pings.
5. At **Ping Interval** enter the interval to be inserted between pings. This is the interval of the ICMP packet. Valid values are **0** to **30** seconds. The default is **1** second.
6. At **Egress Interface (Only for IPv6)**, enter the VLAN ID (VID) of the specific egress IPv6 interface to which the ICMP packet goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not given, PING6 finds the best match interface for destination. Do **not** specify egress interface for loopback address. Do specify egress interface for link-local or multicast address.
7. Click the **Start** button to retrieve the Ping6 output.

After you press the **Start** button, ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed when a reply is received. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

A successful Ping6 result is shown below.

```

PING6 server ff02::2, 56 bytes of data.
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=0, time=10ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=0, time=10ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=1, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=1, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=2, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=2, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=3, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=3, time=0ms
64 bytes from fe80::219:5bff:fe2f:b47: icmp_seq=4, time=0ms
64 bytes from fe80::215:58ff:feed:69dd: icmp_seq=4, time=0ms
Sent 5 packets, received 10 OK, 0 bad

```

You can click the **New Ping** button to re-display the initial Ping6 page.

You can configure the following properties of the issued ICMP packets:

IP Address

The destination IP Address.

Ping Length

The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Ping Count

The count of the ICMP packet. Values range from 1 time to 60 times.

Ping Interval

The interval of the ICMP packet. Values range from 0 second to 30 seconds.

Egress Interface (Only for IPv6)

The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.

When the egress interface is not given, PING6 finds the best match interface for destination.

Do not specify egress interface for loopback address.

Do not specify egress interface for link-local or multicast address.

Buttons

Start: Click to start transmitting ICMP packets.

New Ping: Click to re-start diagnostics with PING.

Messages

% Unable to perform PING6 operation on VLAN 3!

% Please specify correct egress IPv6 interface.

Example

ICMPv6 Ping Output

```

PING6 server ff02::2, 56 bytes of data.
64 bytes from fe80::2c0:f2ff:fe56:1a38: icmp_seq=0, time=10ms
64 bytes from fe80::2c0:f2ff:fe56:1a38: icmp_seq=1, time=0ms
64 bytes from fe80::2c0:f2ff:fe56:1a38: icmp_seq=2, time=0ms
64 bytes from fe80::2c0:f2ff:fe56:1a38: icmp_seq=3, time=0ms
64 bytes from fe80::2c0:f2ff:fe56:1a38: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad

```

New Ping

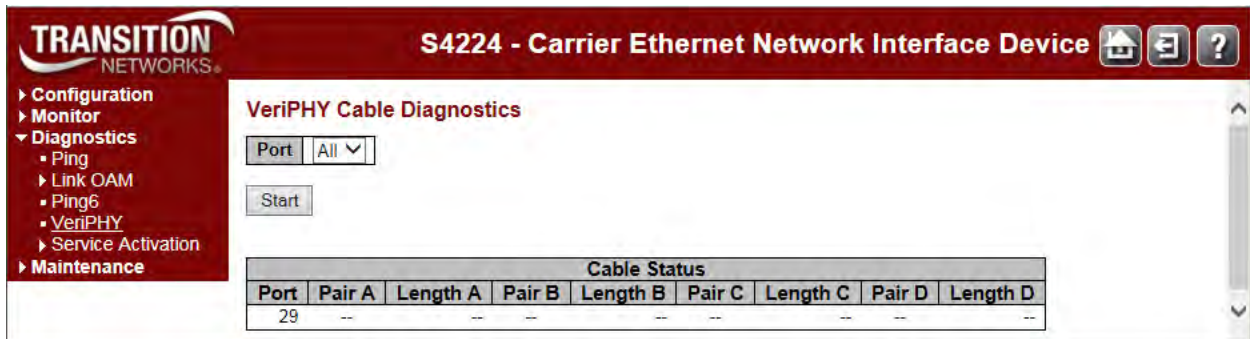
Diagnostics > VeriPHY

This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.

Press the **Start** button to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables 7 - 140 meters long.

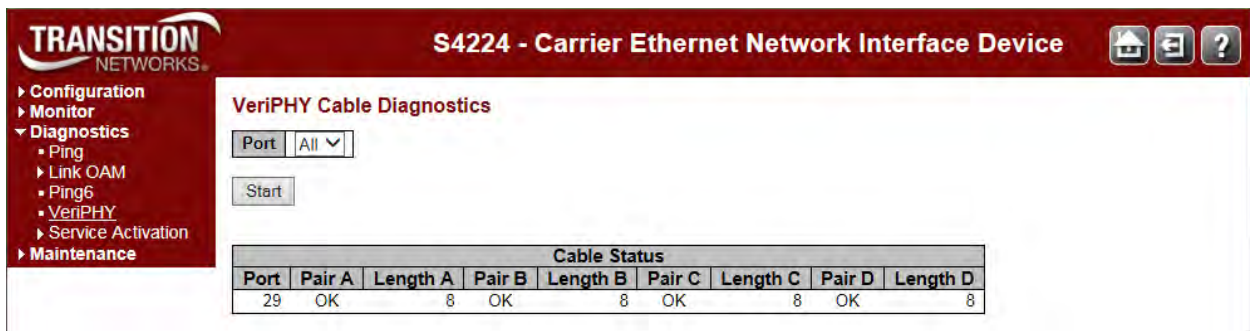
Note: The 10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

The default VeriPHY page is shown below.



While the VeriPHY diagnostic is running, the messages “A network cable is unplugged” and “Switch is currently not responding. Please wait...” display until completion.

A completed VeriPHY page is shown below.



The VeriPHY parameters are described below.

Port

The port for which you are requesting VeriPHY Cable Diagnostics. S4224 ports **All**, **1**, **2**, **3**, and **4** are selectable.

Cable Status

Port: Rge Port number.

Pair: The status of the cable pair. The pair status can be:

OK - Correctly terminated pair

Open - Open pair

Short - Shorted pair

Short A - Cross-pair short to pair A

Short B - Cross-pair short to pair B

Short C - Cross-pair short to pair C

Short D - Cross-pair short to pair D

Cross A - Abnormal cross-pair coupling with pair A

Cross B - Abnormal cross-pair coupling with pair B

Cross C - Abnormal cross-pair coupling with pair C

Cross D - Abnormal cross-pair coupling with pair D

Length: The length (in meters) of the cable pair. The resolution is 3 meters

Messages

Message: *x VeriPHY is running...*

Meaning: The test is in process.

Recovery:

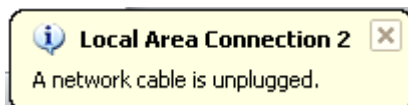
1. Wait for completion or another message.
2. Click the browser's Back button, and then click the Forward button.
3. Contact TN Tech Support if the problem persists.

Message: *Switch is currently not responding. Please wait...*

Meaning: The test has encountered a problem.

Recovery:

1. Wait for completion or another message.
2. Click the browser 'Back' button.
3. Switch to another menu path and then switch back to the **Diagnostics > VeriPHY** menu path.
4. Contact TN Tech Support if the problem persists.



Diagnostics > Service Activation

This page lets you configure and run a Service Activation Test and Loopback Test and save the test results from the **Diagnostics > Service Activation > Test** or from the **Diagnostics > Service Activation > Loopback** menu path. See [Service Activation Configuration](#) section on page 368 for details.

Diagnostics > Service Activation > Test

This page lets you configure and run an Ethernet Service Activation Test and save the test results.



Note: Before running the Service Activation Test, set the shared port mode to **Internal** mode. See [“Configuration > Ports > Shared Port Configuration”](#) on page 29.

1. Make sure the shared port mode is set to **Internal**.
2. At the **Test** dropdown, select the desired Test to run.
3. Click the **Start** button to start the selected test.
4. Click the **Stop** button to stop the selected test.
5. Click the **Show** button to display the test results.
6. Click the **Save report** button to save the test results to a specified location.

Diagnostics > Service Activation > Loopback

The Ethernet Service Activation Testing page lets you activate Loopback on a port. All traffic matching the criteria below will be looped back to the SMAC in the incoming frame. You can activate loopback on a port so that all traffic matching the test criteria will be looped back to the SMAC in the incoming frame.

Note: Policy ID 254 is used for marking traffic. Make sure this Policy ID is not used for other purposes (ECEs) and the ACE Policy Filter is not being used as a bit field that would inadvertently match 254 (i.e., Policy Bitmask should be 0xFF for all ACEs).

The default Ethernet Service Activation Testing page is shown below.

| Ethernet Service Activation Testing | |
|-------------------------------------|-------------------|
| Loopback | |
| State | Inactive |
| Test Side Port | Port 1 |
| SMAC Address | 00-00-00-00-00-01 |
| VLAN ID | 1 |
| Timeout (s) | 300 |

The Loopback test parameters are described below.

State

At the dropdown, set the test state to **Inactive** or **Active**. Note that the Loopback State must be Inactive to change parameters.

Active: Loopback is active. The time remaining active is displayed in the next column (see below).

Inactive: Loopback is inactive

Test Side Port

Select the test side port (the test port where loopback will be enabled). Note that at v 2.2, the S4224 or S4140 cannot be used as an Ethersat loopback device. The workaround is to use an S3280 or other NID as the loopback device.

SMAC Address

The Source MAC Address to match.

VLAN ID

The VLAN ID to match. To match untagged traffic make this value equal to the Port VLAN ID set at **Configuration > VLANs > Port VLAN Configuration**.

Timeout (s)

The timeout value in seconds until loopback automatically becomes inactive. The default is 300 seconds. The valid range is **1-99999999** seconds.

After you set the test parameters and click the **Save** button, the test status displays:

The screenshot shows the web interface for the S4224 - Carrier Ethernet Network Interface Device. The main heading is "Ethernet Service Activation Testing". On the left is a navigation menu with options like GVRP, Service Activation, DDMI, UDLD, Monitor, Diagnostics, and Maintenance. The "Loopback" test is active, as indicated by the "State" dropdown menu. The test parameters are displayed in a table:

| | | |
|----------------|-------------------|----------------------------|
| State | Active | Active Time Remaining: 198 |
| Test Side Port | Port 1 | Frames: 3, Bytes: 402 |
| SMAC Address | 00-00-00-00-00-01 | |
| VLAN ID | 1 | |
| Timeout (s) | 300 | |

Below the table are "Save" and "Reset" buttons. In the top right corner, there is an "Auto-refresh" checkbox and a "Refresh" button.

The test status displays in the format:

Active Time Remaining: 198

Frames: 3, **Bytes:** 402

EtherSAT Messages

Message:

ethersat loopback state set failed. Check that the shared port is internal and try again
etherset loopback testsideport set failed. Check that the shared port is internal and try again
etherset loopback timeout set failed. Check that the shared port is internal and try again
etherset loopback smac set failed. Check that the shared port is internal and try again
etherset loopback vid set failed. Check that the shared port is internal and try again

Meaning: The EtherSAT loopback test failed because the shared port is not set to internal mode.

Recovery: Set the shared port to internal mode using the (config)# command `sharedport internal` and try the loopback test again.

Problem: The S4224 or S4140 cannot be used as an Ethersat loopback device.

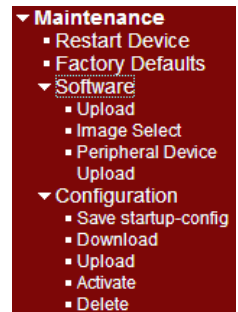
Workaround: Use an S3280 or other NID as the loopback device.

Problem: The 10GE SFP+ ports cannot be set as Test Side Ports. They can be entered and the state set to active but refreshing the page changes them to port 1.

Workaround: Use the 100/1000 SFP ports as Test Side Ports.

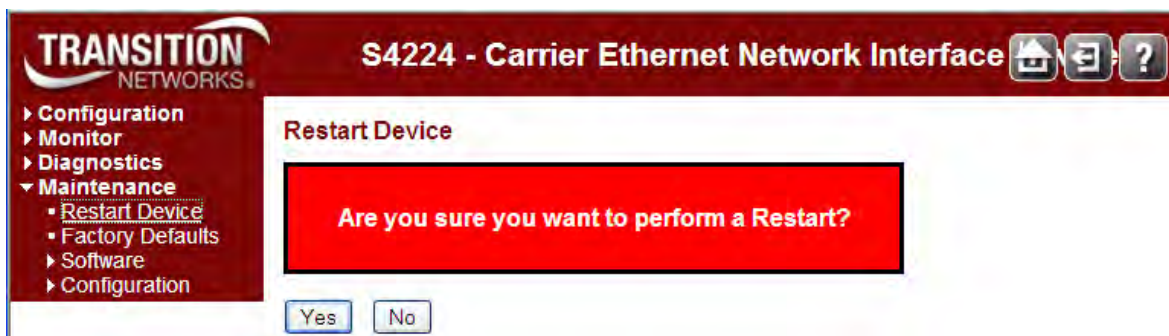
Maintenance Menu

The S4224 **Maintenance** main menu displays the **Restart Device**, **Factory Defaults**, **Software**, and **Configuration** sub-menus as described in the following sections.



Maintenance > Restart Device

You can restart the S4224 from this page.



Procedure

1. Navigate to the **Maintenance > Restart Device** menu path. The confirmation message "Are you sure you want to perform a Restart?" displays.
2. If you are sure you want to restart the S4224, click the **Yes** button.
If you are not sure you want to restart the S4224, click the **No** button and continue operation.
3. To restart the S4224, click the **Yes** button.



The "System restart in progress" screen displays with a series of messages, starting with "Waiting, please stand by ...". When the restart is complete, the S4224 startup screen (**Monitor > Ports > State** page) displays.

Buttons

Yes: Click to restart device.

No: Click to return to the Port State page without restarting.

Maintenance > Restart Device > Force Cool Restart

An error condition may display the **Restart Device** page with an option to force an S4224 cool restart.

If this occurs, at **Maintenance > Restart Device > Are you sure you want to perform a Restart? - Force Cool Restart**, check or uncheck the checkbox and click the **Yes** button.



Restart Device

Are you sure you want to perform a Restart?

Force Cool Restart

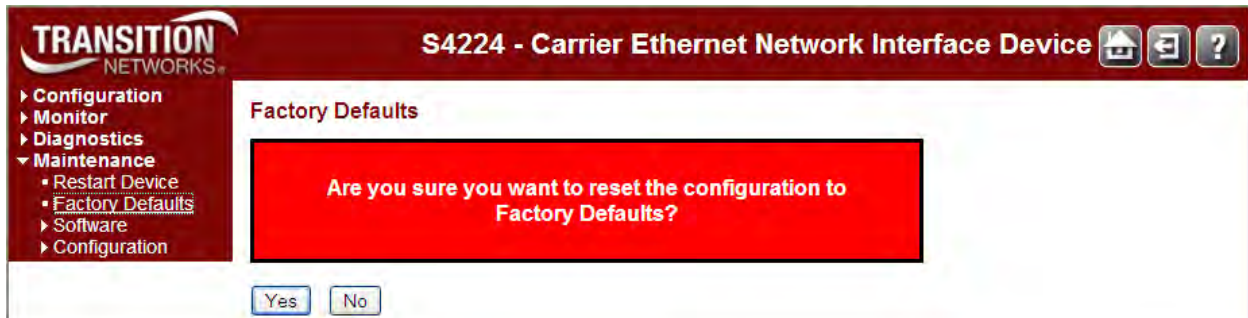
Check the **Force Cool Restart** checkbox and click **Yes** to perform an S4224 cool restart.

Uncheck the **Force Cool Restart** checkbox and click **Yes**, to perform an S4224 cool restart.

Click the **No** button to clear the message without performing any restart.

Maintenance > Factory Defaults

You can reset the S4224 configuration to its factory default settings from this page.



Only the IP configuration is retained after a reset to factory configuration is performed. The new configuration is available immediately, which means that no restart is needed.

Procedure

1. Navigate to the **Maintenance > Factory Defaults** menu path. The confirmation message “*Are you sure you want to reset the configuration to Factory Defaults?*” displays.
2. If you are not sure you want to restart the S4224, click the **No** button and continue operation. If you are sure you want to restart the S4224, click the **Yes** button. The information message “*Configuration Factory Reset Done - The configuration has been reset. The new configuration is available immediately.*” displays.



3. Continue operation.

Buttons

Yes: Click to reset the configuration to Factory Defaults.

No: Click to return to the Port State page without resetting the configuration.

Note: Restoring factory defaults can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot.

In the first minute after reboot, 'loopback' packets are transmitted at port 1. If a 'loopback' packet is received at port 2, the switch will do a restore to defaults.

Maintenance > Software

The S4224 **Maintenance > Software** path lets you select the **Upload**, **Image Select**, and **Peripheral Device** sub-menus.

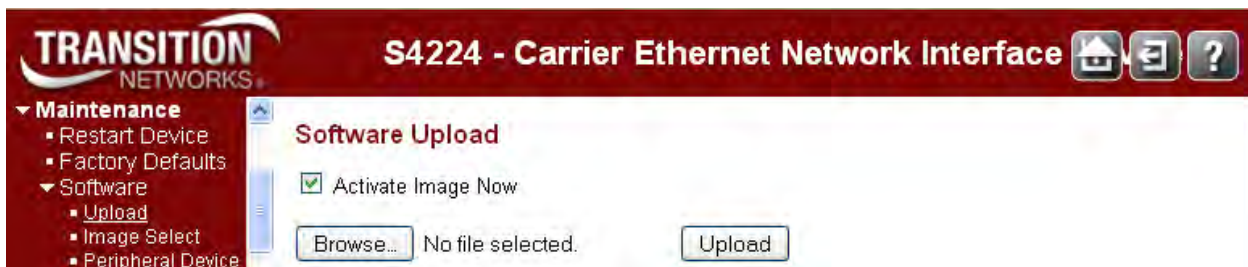
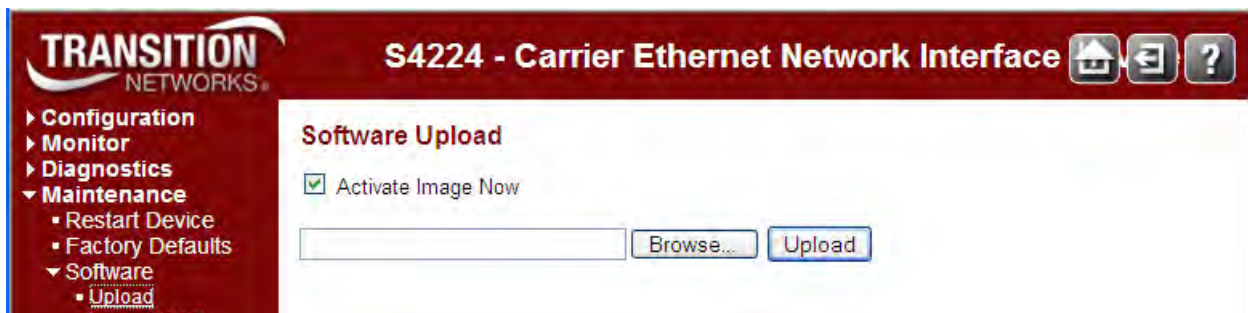
Software Upload via the Maintenance > Software > Upload Path

The S4224 supports firmware upgrade via TFTP and HTTP from the **Maintenance > Software > Upload** path (the Web uses HTTP, and the CLI uses TFTP). All configuration settings are retained when the device resets after successful upgrade operation. The firmware image has a CRC mechanism to prevent a corrupted image to be loaded onto the S4224. The upgrade procedure handles error conditions such as a network disruption during upgrade, power outages, TFTP/HTTP connection issues, etc. and will continue to operate using the installed image in case of upgrade failures.

Note: It is a good idea to create a backup of the configuration before upgrading the firmware.

Note: An upgrade from v 1.9 or earlier to v 2.2.x will result in loss of config settings.

The S4224 does not disrupt any data plane traffic during the image download process; the data traffic will experience a loss when the device resets to boot with the new image, but the service is restored immediately after the S4224 is configured. The *.dat* file contains a checksum which is validated after upload. If power outage occurs while writing the flash, the flash upgrade will fail. This is why there is an alternate image to serve as an alternate or replacement file. The Software Upload page is shown below in MS Windows (top) and Mozilla Firefox.



This page lets you update the S4224 firmware.

Warning: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. **Do not restart or power off the device at this time** or the S4224 may fail to function afterwards.

Activate Image Now : Check to activate and reboot immediately. Uncheck to activate the image manually later. By default the image will not be activated and the device will not reboot.

Browse to the location of a software image and click the **Upload** button.

After the software image is uploaded, a page announces that the firmware update is initiated.

After about a minute, the firmware is updated.

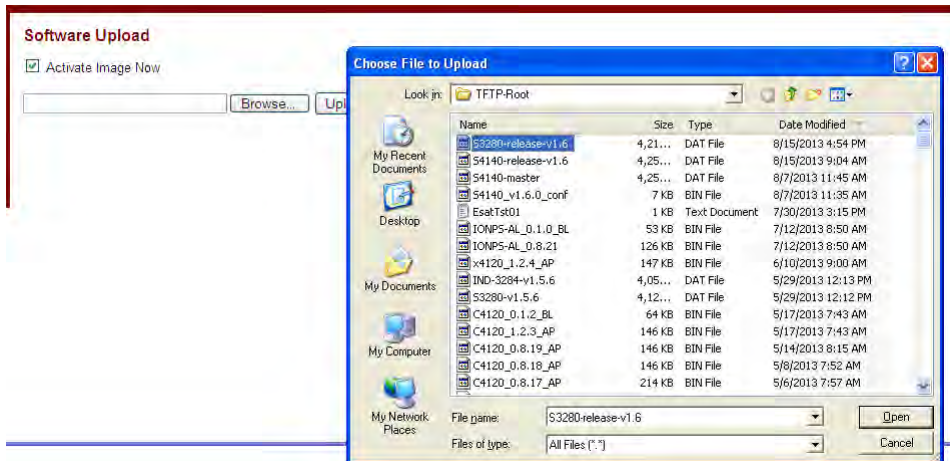
If "Activate Image Now" is checked, then all managed switches in the stack will automatically reboot. the switch will automatically reboot.

If "Activate Image Now" was not checked, you will be redirected to the image selection page to manually select the new image.

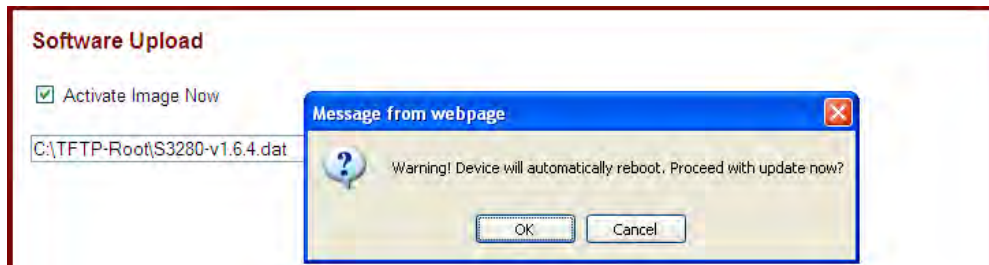
Software Upload Procedure

This procedure transfers the uploaded firmware image to the S4224 flash component. You have the option to activate the image immediately or later. **Note:** do not reset or power off the S4224 during this process.

1. Navigate to the **Maintenance > Software > Upload** menu path.
2. Click the **Browse** button. The "Choose File to Upload" dialog displays.



3. Browse to the location of a software image, select a file name with a **.DAT File** extension, and click the **Open** button.
4. At the **Activate Image Now** checkbox, check or uncheck the box:
 - If you leave the checkbox unchecked, the image will be uploaded, but not immediately activated.
 - If you check the checkbox, the image will be uploaded, and can be immediately activated.
5. Click the **Upload** button. The confirmation dialog "*Warning! Device will automatically reboot. Proceed with update now?*" displays.
 - If the upload version already is installed, the message "*Firmware Upload Error - Flash is already updated with this image*" displays. Click the browser Back button to recover.



Note: do not reset or power off the S4224 until this firmware update procedure completes.

6. Click **OK** to proceed with the update, or click **Cancel** to return to the Firmware Update page. After the software image is uploaded, a page announces that the firmware update is initiated.

Note: do not reset or power off the S4224 during this process.

If you checked the **Activate Image Now** checkbox, the message “*The upload firmware image is being transferred to flash. The system will restart after the update. Until then, do not reset or power off the device!*” displays.



If you unchecked the **Activate Image Now** checkbox, the message “*Writing firmware image to flash. Do not reset or power off the device!*” displays.



7. The “*Flashing, please wait ...*” series of messages display during the process. After 1-2 minutes, the firmware is updated.

If you checked the **Activate Image Now** checkbox, the S4224 restarts. When the S4224 startup screen displays, continue operation.

If you unchecked the **Activate Image Now** checkbox, the **Software Image Selection** page displays. Continue with the **Image Select** procedure below.

Messages:

Do not reset or power off the device!

Error: Incomplete stack update - update aborted

FIRMWARE_ERROR_xxx code

Flashing, please wait...

Flash is already updated with this image

Programming, please wait ...

Rebooting system...

Restarting, please wait...

Slave, only doing local update

The uploaded firmware image is invalid. Please use a correct firmware image.

Waiting for firmware update to complete

(Still) waiting for firmware update to complete

Warning! Device will automatically reboot. Proceed with update now?

Maintenance > Software > Image Select

This page provides information about the Active (current) and Alternate (backup) firmware images in the device, and allows you to revert to the Alternate Image.

TRANSITION NETWORKS S4224 - Carrier Ethernet Network Interface Device

▶ Configuration
 ▶ Monitor
 ▶ Diagnostics
 ▼ Maintenance

- Restart Device
- Factory Defaults
- ▼ Software
 - Upload
 - Image Select
 - Peripheral Device Upload
- ▶ Configuration

Software Image Selection

| Active Image | |
|--------------|---------------------------|
| Image | managed |
| Version | S4224 (standalone) 2.2.1 |
| Date | 2015-07-15T22:11:55-05:00 |

| Alternate Image | |
|-----------------|---------------------------|
| Image | managed.bk |
| Version | S4224 (standalone) 2.2.0 |
| Date | 2015-07-14T22:12:04-05:00 |

The Software Image Selection page displays two tables with information about the **Active Image** and the **Alternate Image**.

Note:

1. If the Active Image firmware image is the same as the Alternate image, only the "Active Image" table displays. In this case, the **Activate Alternate Image** button is also disabled.
2. If the Alternate Image is active (due to a corruption of the primary image or due to manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.

Image

The flash index name of the firmware image. The name of the primary (existing / preferred) image is **managed**, the alternate image is named **managed.bk**.

Version

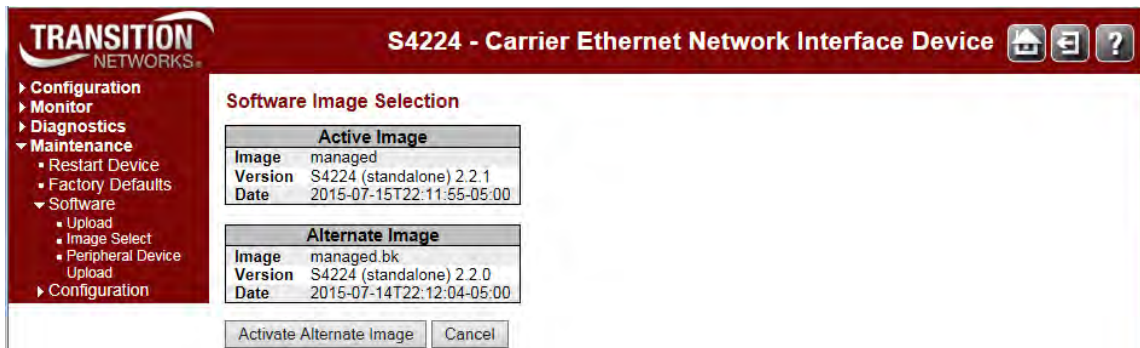
The version of the firmware image (e.g., **S4224-24 (standalone) 2.2.1** as shown above).

Date

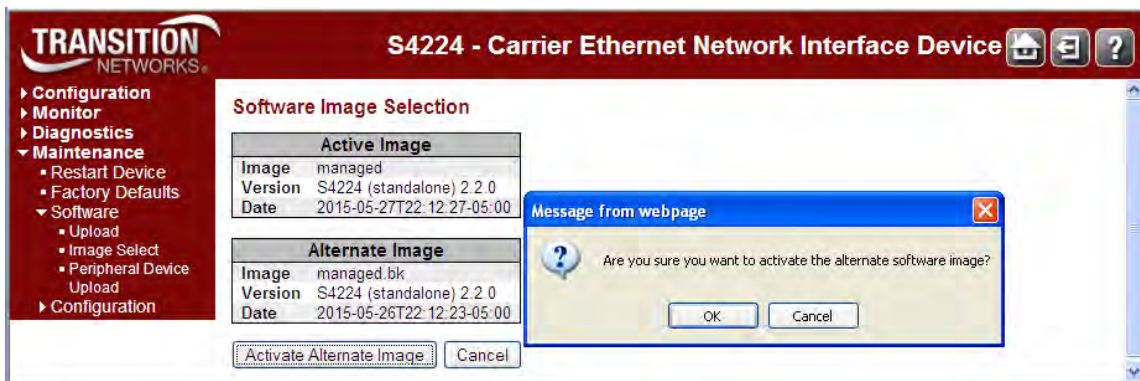
The date when the firmware was produced (e.g., **2015-07-15T22:11:55-05:00** as shown above).

Image Select Procedure (Activate Alternate Image)

1. Navigate to the **Maintenance > Software > Image Select** menu path.



2. Click the **Activate Alternate Image** button. A confirmation message displays:



3. If you are not sure you want to activate the alternate S4224 image, click the **Cancel** button and continue operation.
If you are sure you want to restart the S4224, click the **OK** button. The S4224 restarts and displays the "System restart in progress" message as shown below:



All of the front panel 100/1000 SFP LEDs light momentarily.

4. When the S4224 startup screen (**Monitor > Ports > State**) displays, continue operation.

Buttons

Activate Alternate Image: Click to use the alternate image. This button may be disabled depending on system state.

Cancel: Cancel activating the backup image; navigates away from this page.

Messages

Messages:

Activate image (swap) now and reboot
Activate image (swap) manually later
Alternate image activated, now rebooting.
Alternate image activation failed.

Message: *System config has just converted to a new format. Please backup the configuration if needed.*

CLI Commands to Re-Access the Web GUI

After a Software Upload via the **Maintenance > Software > Upload** path, you can use the following CLI commands to regain web GUI access:

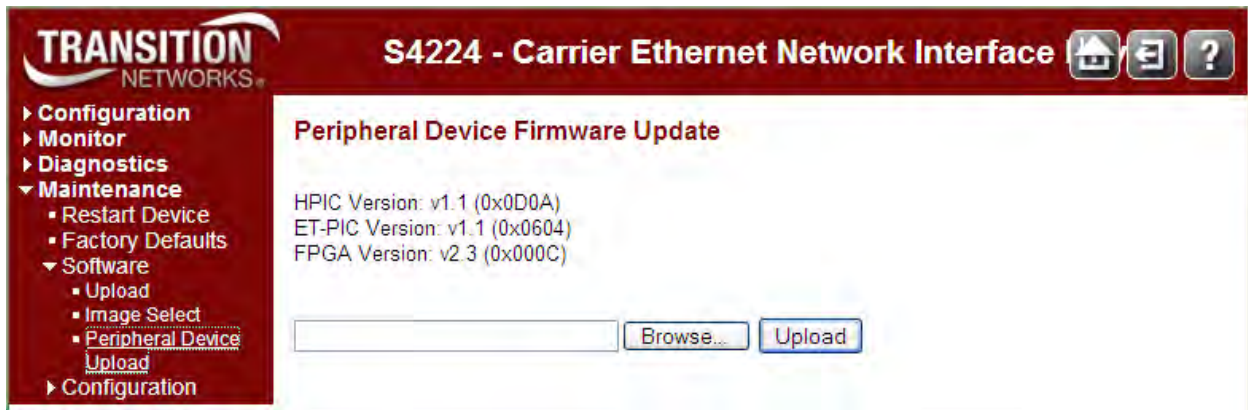
```
# show ip int brief
Vlan Address                Method  Status
-----
# conf term
(config)# int vlan 1
(config-if-vlan)# ip addr 192.168.1.110 255.255.255.0
(config-if-vlan)# end
# show ip int brief
Vlan Address                Method  Status
-----
  1 192.168.1.110/24        Manual  UP
#
```

You can then access the web GUI via the IP address and netmask entered (e.g., 192.168.1.110 and 255.255.255.0 in the example above). See the S4224 CLI Reference manual for details.

Maintenance > Software > Peripheral Device Upload

This page lets you update peripheral device firmware if present.

Peripheral Device Firmware Update



Browse to the location of a firmware image and click Upload.

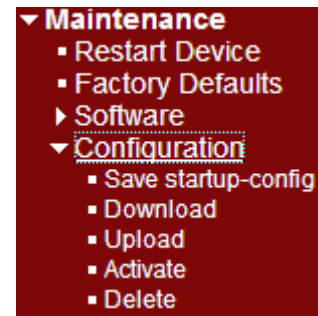
After the firmware image is uploaded, a page announces that the firmware update is initiated. The switch will automatically reboot when the firmware update is complete.

Warning: While the firmware is being updated, Web access appears to be defunct. **Do not restart or power off the device at this time** or the switch may fail to function afterwards.

Maintenance > Configuration

This section covers config file handling via the **Maintenance > Configuration** menu path, including how to:

1. Save the config that is currently running
2. Download a different config file
3. Upload the downloaded config file
4. Activate an uploaded config file
5. Delete an inactive config file



Industry-standard Configuration Support

The S4224 supports an industry-standard configuration where the commands are stored in a text format.

The S4224 stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.

The three system files are:

running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.

startup-config: The startup configuration for the switch, read at boot time.

default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings. This is a per-build customizable file that does not require source code changes.

It is also possible to store up to two other files and apply them to the running-config, thereby switching configuration. The maximum number of files in the configuration file is limited to a compressed size which does not exceed approximately 1MB.

The configuration made can be dynamically viewed by entering the `show running-config` command. This current running configuration may be copied to the startup configuration using the `copy` command.

This industry-standard file may be edited and can be populated on multiple other switches using any standard text editor offline.

Save Running Config to Startup-Config

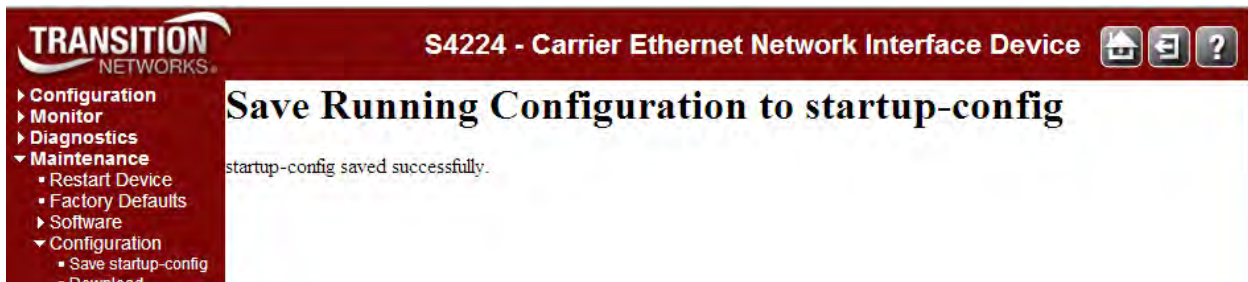
The **Maintenance > Configuration > Save startup-config** menu path lets you copy the *running-config* to *startup-config*, thereby ensuring that the currently active configuration will be used at the next reboot.

Note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

1. Navigate to the **Maintenance > Configuration > Save startup-config** menu path.



2. Click the **Save Configuration** button. When done, the message *startup-config saved successfully* displays.



3. Select any menu option and continue operation.

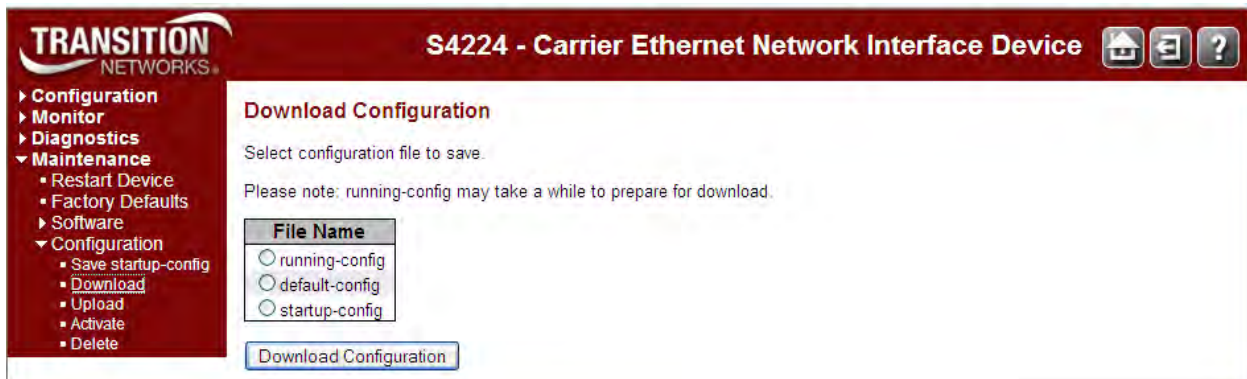
Download Configuration File

The **Maintenance > Configuration > Download** menu path lets you download a selected configuration file. The defaults include the *running-config*, *default-config* and the *startup-config*.

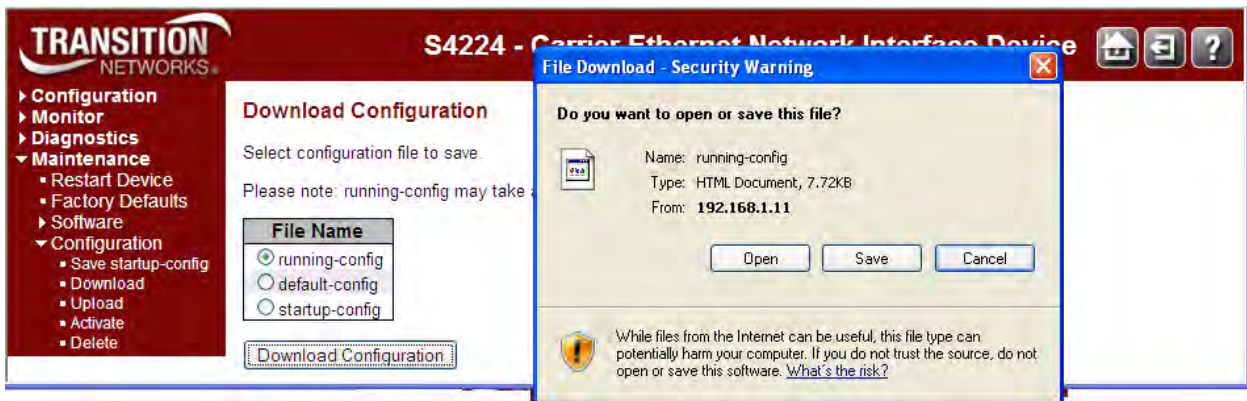
| File Name | |
|-----------------------|----------------|
| <input type="radio"/> | running-config |
| <input type="radio"/> | default-config |
| <input type="radio"/> | startup-config |

Note that the download of a *running-config* may take a little while to complete, as the file must be prepared for download.

1. Navigate to the **Maintenance > Configuration > Download** menu path.
2. Select the file to save and click the **Download Configuration** button.



3. At the *File Download* dialog, click the **Save** button.



4. At the *Save As* dialog, select the Save In location and click the **Save** button.
5. At the *Download Complete* dialog, click the **Close** button. The file is saved to the specified location.

Note: At the *File Download* dialog, the config files can also be opened. The Default configuration file is read and applied immediately after the system configuration is reset to default. The file is read-only and cannot be modified.

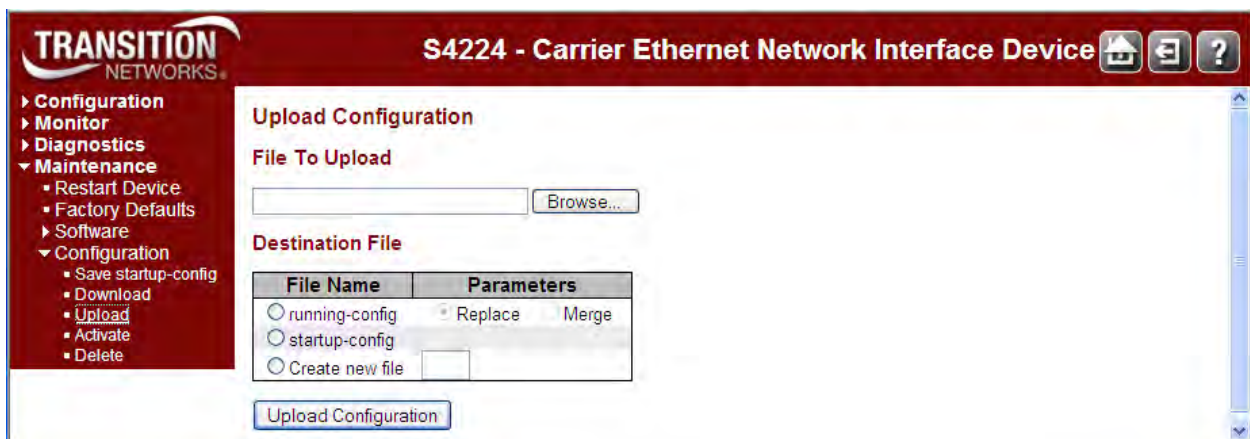
Upload a Configuration File

You can upload a file from the web browser to all the files on the switch (except *default-config*, which is read-only). If the destination is *running-config*, the file will be applied to the switch configuration. This can be done in two ways:

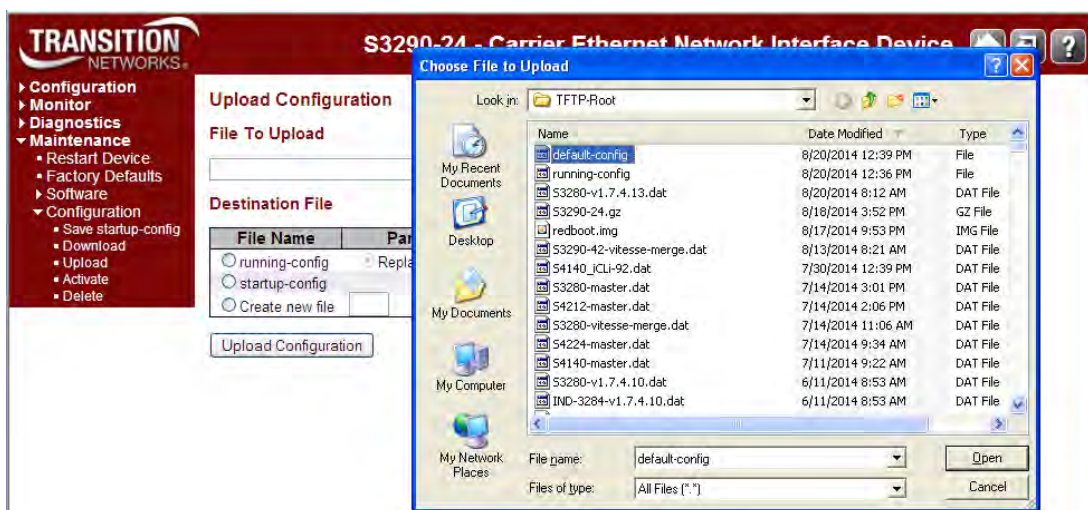
- **Replace** mode: The current configuration is fully replaced with the configuration in the uploaded file.
- **Merge** mode: The uploaded file is merged into running-config.

If the file system is full (i.e., contains the three system files mentioned above plus other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.

1. Navigate to the **Maintenance > Configuration > Upload** menu path to display the Upload Configuration page.

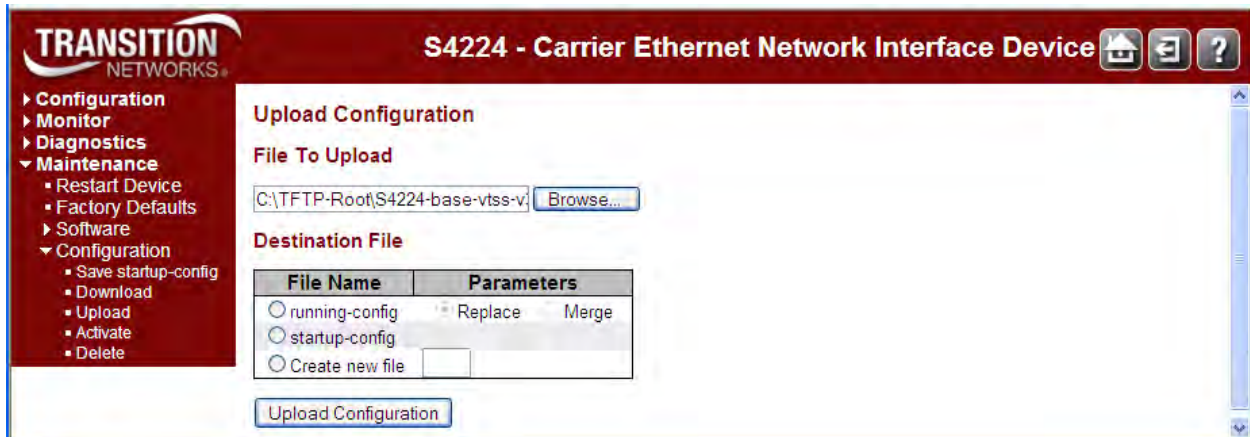


2. Click the **Browse** button to display the *Choose File to Upload* dialog.



3. Select the desired file and click the **Open** button.

The Upload Configuration page displays again with the selected file to upload:



4. Select the Destination File Name.

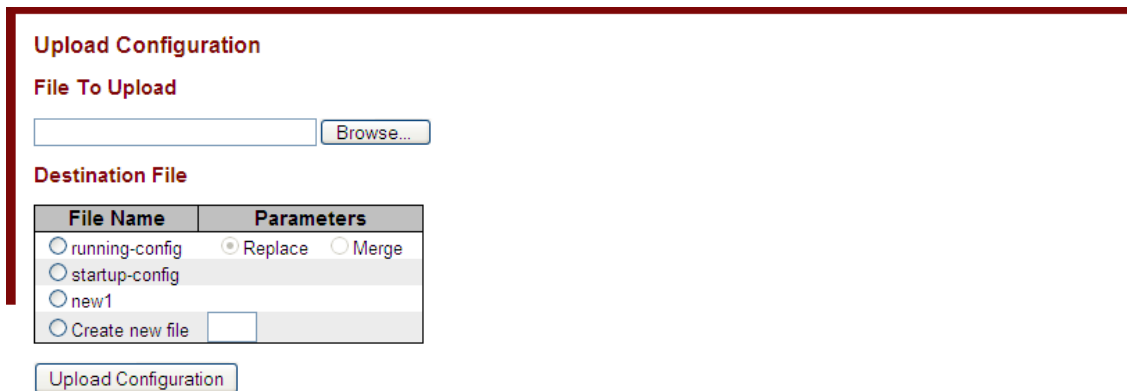
If the destination is **running-config**, the file will be applied to the S4224 configuration. This can be done in two ways:

Replace: The current configuration is fully replaced with the configuration in the uploaded file.

Merge: The uploaded file is merged into running-config.

If the file system is full (i.e., contains the three system files mentioned above plus two other files), it is not possible to create new files, but an existing file must be overwritten or another deleted first.

5. At the Choose File dialog, click the **Open** button.
6. Click the **Upload Configuration** button.
7. If the upload is successful, the message *Upload successfully completed.* displays.
8. Click the Browser's Back button to continue. The Upload Configuration page displays again with the uploaded file (e.g., *new1* in the screen below). The Download Configuration page will also display the uploaded file.



Message: If the message *Missing file name parameter* displays, click the Browser's Back button and enter a file name.

Message: If the message *"Please select a source file."* displays, click the **OK** button to clear the webpage message and Browse to and select a File To Upload.

Activate a Configuration File

You can activate any of the configuration files present on the S4224, except for the *running-config* file, which represents the currently active configuration.

Note: the previous configuration will be completely replaced, potentially leading to loss of management connectivity. **Note:** If the configuration changes IP settings, management connectivity may be lost.

1. Navigate to the **Maintenance > Configuration > Upload** menu path to display the Upload Configuration page.
2. Select the configuration file to activate and click the **Activate Configuration** button. This will initiate the process of completely replacing the existing configuration with that of the selected file.

The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Note that the activated configuration file will not be saved to *startup-config* automatically.

Messages: at the Activating New Configuration page:

Please note: If the configuration changes IP settings, management connectivity may be lost.

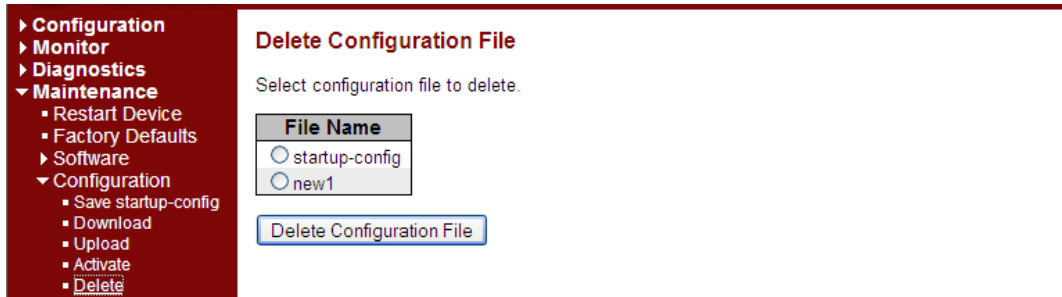
Status Activation completed successfully.

Output Status Activation completed successfully.

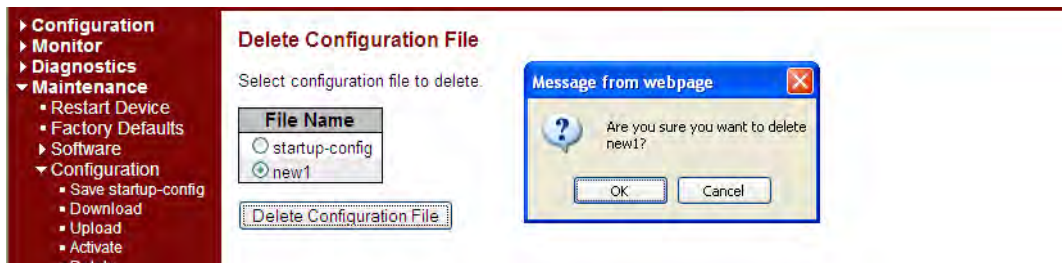
Delete a Configuration File

You can delete any of the writable files stored in flash, including *startup-config*. If this is done and the switch is rebooted without a prior Save operation, the switch resets to its default configuration.

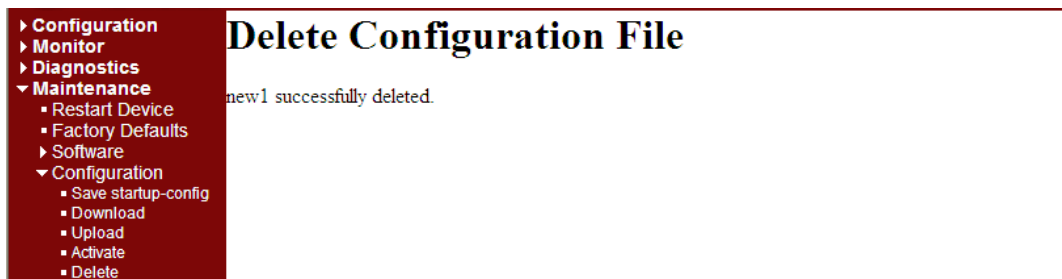
1. Navigate to the **Maintenance > Configuration > Delete** menu path to display the Delete Configuration page.



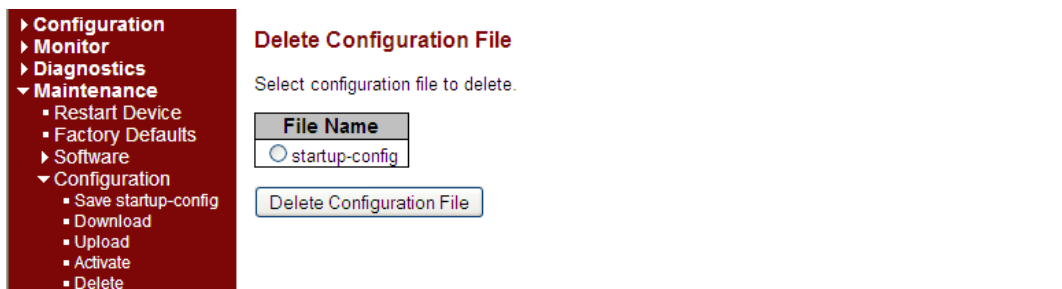
2. Select the filename of the config file to be deleted.
3. Click the **Delete Configuration File** button. A confirmation message displays.



4. Click the **OK** button to clear the webpage message. If successfully deleted, a confirmation page displays.



5. Click the Browser's Back button. The Delete Configuration File page displays again with the selected config file deleted:



6. Continue operation.

3. Messages and Troubleshooting

This section provides general and specific S4224 problem solving suggestions, general error recovery steps, and specific web interface messages, meanings, examples, and possible recovery steps.

S4224 Troubleshooting

1. Check the S4224 Back Panel Connections (see the S4224 Install Guide).
2. Verify the Installation. Check the Operating System, Web Browser, Telnet Client, and/or Terminal Emulation package support (see the S4224 Install Guide).
3. Make sure your particular model supports the function attempted.
4. Check the S4224 Front Panel Connectors and LEDs (see the S4224 Install Guide).
5. Respond to any S4224 error messages (see “S4224 Error Recovery” below).
6. Run the S4224 Diagnostics tests and verification functions (e.g., Ping, Link OAM Mib Retrieve, Ping6, VeriPHY). See the “[Diagnostics Main Menu](#)” section on page 521.
7. Perform the S4224 troubleshooting and service functions (e.g., Restart Device, reset to Factory Defaults, Software Upload, Image Select). See the “[Maintenance Menu](#)” section on page 531.
8. Check the S4224 operating parameters (e.g., Information, CPU Load, Log, Detailed Log). See the “[Monitor](#)” section on page 380.
9. In Windows Internet Explorer, try clicking the **Tools > Compatibility View** option.
10. If you can access the S4224 via PuTTY or HyperTerminal but not via the web interface, enter the **reload defaults keep-ip** CLI command and try accessing the S4224 web interface again.

EPS Troubleshooting

Provisioning Mismatches

With all of the options for provisioning of protection groups, there are opportunities for mismatches between the provisioning at the two ends. These provisioning mismatches take one of several forms:

- Mismatches where proper operation is not possible.
- Mismatches where one or both sides can adapt their operation to provide a degree of interworking in spite of the mismatch.
- Mismatches that do not prevent interworking.

Not all provisioning mismatches can be conveyed and detected by information passed through the APS communication. There are too many combinations of valid entity numbers to easily provide full visibility of all of the configuration options.

Generally, selecting revertive / non-revertive operation is the same at both ends of the protection group. However, a mismatch of the revertive / non-revertive parameter does not prevent interworking. See Recommendation ITU-T G.8031/Y.1342 for specifics on linear protection switching for Ethernet Virtual Local Area Network (VLAN) signals.

Request State Priorities

| <u>Request / State</u> | <u>Priority</u> |
|--|-----------------|
| 1111 Lockout of protection (LO) | |
| 1110 Signal fail for protection (SF-P) | Highest |
| 1101 Forced switch (FS) | ^ |
| 1011 Signal fail for working (SF) | |
| 1001 Signal degrade (SD) (Note) | |
| 0111 Manual switch (MS) | |
| 0110 Manual switch to working (MS-W) | |
| 0101 Wait to restore (WTR) | |
| 0100 Exercise (EXER) | |
| 0010 Reverse request (RR) | |
| 0001 Do not revert (DNR) | v |
| 0000 No request (NR) | Lowest |

Note: SF-P (Signal fail on the protection transport entity) is a higher priority than any defect that would cause a normal traffic signal to be selected from protection.

Protection Types

The valid protection types are:

- 000x 1+1** Unidirectional, no APS communication
- 100x 1+1** Unidirectional w/APS communication
- 101x 1+1** Bidirectional w/APS communication
- 111x 1:1** Bidirectional w/APS communication

The values are chosen such that the default value (all zeros) matches the only type of protection that can operate without APS (1+1 unidirectional).

Note that 010x, 001x and 011x are invalid since 1:1 and bidirectional require an APS communication.

If the "B" bit mismatches, the selector is released since 1:1 and 1+1 are incompatible, resulting in a defect.

If the "B" bit matches:

- If the "A" bit mismatches, the side expecting APS will fall back to 1+1 unidirectional switching without APS communication.
- If the "D" bit mismatches, the bidirectional side will fall back to unidirectional switching.
- If the "R" bit mismatches, one side will clear switches to "WTR"

Failure of Protocol Defects

The "Failure of protocol" situations for protection types requiring APS include:

- Fully incompatible provisioning (the "B" bit mismatch)
- Working/protection configuration mismatch.
- Lack of response to a bridge request (i.e., no match in sent "requested signal" and received "requested signal") for >50ms.

Fully incompatible provisionings and working/protection configuration mismatches are detected by receiving a single APS frame.

Detecting and clearing "failure of protocol" defects are defined in ITU-T G.8021.

Any received 'unknown request' or any 'request for an invalid signal number' is ignored.

ERPS Troubleshooting

Failure of protocol defect: due to errors in provisioning, the ERP control process may detect a combination of conditions which should not occur during "normal" conditions. To warn the operator of such an event, a failure of protocol – provisioning mismatch (FOP-PM) is defined. The FOP-PM defect, detected if the RPL owner node receives one or more No Request R-APS message(s) with the RPL Blocked status flag set (NR, RB), and a node ID that differs from its own. The ERP control process must notify the equipment fault management process when it detects such a defect condition, and continue its operation as well as possible. This is only an overview of the defect condition. The associated defect and its details are defined in [ITU-T G.8021](#) as amended by its Amendments 1 and 2.

IPv6 Troubleshooting

Start by using these third party resources when performing general IPv6 problem solving:

- The standard Windows 7 command-line tools with full IPv6 functionality (Ping, Ipconfig, Pathping, Tracert, Netstat, and Route all support IPv6).
- The IPv6-specific tools in the Netsh command.

Address Resolution in Windows 7

In unicast global IPv6 (equal to IPv4 Public) addresses, the 64-bit host portion of the address is derived from the MAC address of the network adapter. The Neighbor Discovery (ND) protocol resolves IPv6 addresses to MAC addresses. The resolution of host names to IPv6 addresses is done by DNS with the exception of link-local (equivalent to IPv4 APIPA) addresses, which resolve automatically. DNS handles records for IPv6 host names similar to IPv4 and also uses pointer (PTR) records to perform reverse lookups. Where DNS is not implemented (e.g., peer-to-peer environments) the Peer Name Resolution Protocol (PNRP) provides dynamic name registration and name resolution.

Verify IPv6 Configuration in Windows 7

The main tool is Ipconfig. The command **ipconfig /all** displays both IPv4 and IPv6 configuration. To display the configuration of only the IPv6 interfaces use netsh. The **netsh interface ipv6 show address** command displays each interface IPv6 address including the interface ID after the % character (the configuration can be accessed via the GUI).

Verify IPv6 Connectivity

ping the local address. Note that if pinging link-local addresses from one host to another, you must include the destination adapter interface ID (e.g., ping fe80::38e7:3df1:f5ff:fd0%13). When pinging site-local (equal to IPv4 Private) addresses you can add the interface ID to ensure that the address is configured on the desired interface. You must add an 'allow' rule for ICMPv6 traffic to pass through each computer's firewall.

Command examples - third party CLI commands for IPv6:

```
ipconfig /all
netsh interface ipv6 show address
ping fe80::38e7:3df1:f5ff:fd0%13)
netsh interface ipv6 delete neighbors
netsh interface ipv6 show neighbors
netsh interface ipv6 delete destinationcache
netsh interface ipv6 show destinationcache
netsh interface ipv6 show route
route print
tracert -d <destination IPv6 address>
pathping -d <destination IPv6 address>
```

For Additional Information

IPv6 Forum at <http://www.ipv6forum.com/>

ARIN (American Registry for Internet Numbers) at https://www.arin.net/knowledge/ipv6_info_center.html
or ARIN wiki at http://www.getipv6.info/index.php/Main_Page

Cisco: <http://www.ciscopress.com/articles/article.asp?p=777892&seqNum=7>

Troubleshooting IPv6 on Windows 7: <http://itexpertvoice.com/home/troubleshooting-ipv6-on-windows-7-and-why-its-worth-the-bother/>

Troubleshooting IPv6 on Windows Servers (Microsoft TechNet): [http://technet.microsoft.com/en-us/library/cc780623\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc780623(WS.10).aspx)

IPv6 Auto Config Troubleshooting

Determine whether your particular computer will require reconfiguration. For example, for Microsoft .NET Framework version 2.0 and later, IPv6 is enabled by default. For .NET Framework version 1.1 and earlier, IPv6 is disabled by default. For more information see the MSDN article at <http://msdn.microsoft.com/en-us/library/8db2058t.aspx>. Windows Server 2008 provides complete support for IPv6 and all of its features, and does not need additional installation or configuration.

For Windows 7 see <http://technet.microsoft.com/en-us/magazine/2009.07.cableguy.aspx>.

For Windows XP see <http://support.microsoft.com/kb/2478747>.

For Windows Vista see <http://ipv6.com/articles/general/IPv6-Microsoft-Vista.htm>.

For Linux / BSD, see <http://ipv6.com/articles/applications/Linux-and-BSD.htm> or http://tldp.org/HOWTO/html_single/Linux+IPv6-HOWTO/ or your distribution documentation and/or website.

RADIUS Troubleshooting in Windows Server Environments

Microsoft RADIUS implementations differ between Windows Server 2003 and Windows Server 2008.

Windows Server 2003: Internet Authentication Service (IAS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy in Windows Server 2003.

As a RADIUS server, IAS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless and virtual private network (VPN) connections.

As a RADIUS proxy, IAS forwards authentication and accounting messages to other RADIUS servers.

In Windows Server 2008, IAS was replaced with Network Policy Server (NPS).

See <http://technet.microsoft.com/en-us/network/bb643123> for more information.

Windows Server 2008: Network Policy Server (NPS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy in Windows Server 2008. NPS is the replacement for Internet Authentication Service (IAS) in Windows Server 2003. (NPS is actually more than a replacement for IAS, it does what IAS did and much more.) As a RADIUS server, NPS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless and virtual private network (VPN) connections. As a RADIUS proxy, NPS forwards authentication and accounting messages to other RADIUS servers. NPS also acts as a health evaluation server for Network Access Protection (NAP).

See <http://technet.microsoft.com/en-us/network/bb629414.aspx> for more information.

Configure FreeRadius or TACACS+ for Correct ADMIN Level

AAA 'keyword attribute'

Problem: When the privilege Levels with the Radius Account to the switch are not sent, you have read-only access. FreeRadius is sending Privilege Level 5 per the default. (This also applies to TACACS+ with *service=shell* and *priv-lvl=x*.)

Meaning: If the S4224 does not see these *attrs* then it defaults to level 1 (minimal access). The S4224 can do vendor specific values of Cisco and Zyxel:

```
Vendor-id: 9 (Cisco) Vendor-type: 1
Vendor-id: 890 (Zyxel) Vendor-type: 3
```

FreeRadius sends a Privilege Level 5 by default. The Keyword or attribute for Transition is *vendor_value* syntax: "*shell:priv-lvl=x*" where x is an integer from 0 to 15. For Extreme it is 'Extreme-CLI-Authorization', for ADVA DWDM 'ADVA-ADMIN', for other vendors, something else (e.g., the config for Extreme Switches is *Extreme-CLI-Authorization = 1*).

Recovery:

1. The current security privilege setting for the user must be 15. The S4224 range is 1 to 15 (where 15 is the highest value / fullest possible access to all S4224 functions).
2. See "[AAA Configuration](#)" on page 119 of the Web User Guide for more information on configuring via the web interface. See the "[Security AAA commands](#)" section of the CLI Command Reference for more information on configuring via the CLI. See the **Configuration > Security > Switch > Privilege Levels** menu path. See the "[Security Switch Users](#)" commands section.
3. This works similarly for TACACS+ with *service=shell* and *priv-lvl=x*.

FreeRADIUS includes a RADIUS server, a BSD licensed client library, a PAM library, and an Apache module. The word 'FreeRADIUS' usually refers to the RADIUS server. FreeRADIUS is the most widely deployed RADIUS server in the world, and it is the basis for several commercial offerings. FreeRADIUS supplies the AAA needs of many Fortune-500 companies and Tier 1 ISPs.

FreeRADIUS supports a simple processing language in its configuration files, called "un-language". The goal of the language is to allow simple policies to be written with minimal effort. Those policies are then applied when a request is being processed. Requests are processed through virtual servers (including the default one), in the sections titled "authorize", "authenticate", "post-auth", "preacct", "accounting", "pre-proxy", "post-proxy", and "session". The keywords for the language are a combination of pre-defined keywords and references to loadable module names. Subject to a few limitations, any keyword can appear in any context. The language consists of a series of entries, each one with one line. Each entry begins with a keyword and entries are organized into lists. The language is processed line by line, from the start of the list to the end. Actions are executed per-keyword.

For the FreeRADIUS "RADIUS Attribute List" see <http://freeradius.org/rfc/attributes.html>. See <http://freeradius.org/radiusd/man/unlang.html> for the FreeRADIUS "unlang - FreeRADIUS Processing un-language" page. The FreeRADIUS Version 2 Documentation page is at <http://freeradius.org/doc/>.

TACACS+ (and RADIUS) have generally replaced the earlier protocols in more current networks. TACACS+ uses TCP and RADIUS uses UDP; some administrators recommend TACACS+ because TCP is considered more reliable. While RADIUS combines authentication and authorization in a user profile, TACACS+ separates the two operations. TACACS+ is available from Cisco, shrubbery.net, rubyforge.org and others.

Troubleshooting High CPU Load Conditions

After the S4224 completes the boot process, the switch CPU performs two distinct functions simultaneously: it runs the various system processes required for a networked switch, and it sends / receives packets to / from the S4224 hardware. CPU load increases when a system process requires more time or when more network packets are sent and received. Under normal operating conditions, the CPU is busy at least 5 percent of the time.

Since background S4224 processes on its switch timers execute multiple times per second, the S4224 never reports CPU utilization at 0%, even for very simple deployments. Normal data traffic packet switching is done in the S4224 hardware without involving the CPU, so it is not affected by an overly busy CPU.

The CPU becomes too busy when it receives too many packets from the S4224 hardware or when a system process consumes too much CPU time. When either of these functions uses CPU resources to the detriment of the other, the CPU becomes "too busy". For example, if the CPU is receiving numerous packets because of a broadcast storm on the network, it becomes so busy processing all of the packets that other system processes do not have access to CPU resources.

In many instances, high CPU load is normal and does not cause network problems. High CPU utilization becomes a problem when the S4224 fails to perform as expected. CPU utilization spikes caused by a known network event or activity are not problems (even an 85% spike may be acceptable, depending on the cause).

Over time, the switch operates within a certain sustained CPU load range, which is considered the normal operations baseline. You can use the output of the **system load** CLI command or the **Monitor > System > CPU Load** menu path.

The CPU Load percentage is shown at 100 ms, 1 second, and 10 second intervals. All numbers represent running averages. Note that the web interface has an Auto-refresh checkbox to refresh the page automatically every 3 seconds.

Frequent unexplained spikes to the established normal operating baseline, or sudden utilization jumps with no explanations are likely causes for concern.

Below are some common symptoms of high CPU utilization.

- High percentages in the CLI command output or web interface graph: check the output of the **system load** CLI command.
- Slow performance: services fail to respond (e.g., slow Telnet response or unable to Telnet to the S4224; slow console response, slow or no ping response).

If you notice any of these symptoms, follow the steps below to alleviate the problem.

1. Check for a possible security issue. A high CPU utilization can be caused by a security issue, such as a worm or virus in your network. This is especially likely if there have not been recent changes to the network. A configuration change (e.g., adding additional lines to ACLs) can mitigate the effects of this problem.
2. Collect more information using the show version of the CLI commands (e.g., system config, system log, etc.).
3. If the S4224 is accessible and you can reproduce the problem, try cycling power to the S4224.
4. Try lowering or disabling all sys logging. Increase logging buffer size.
5. Make sure any debug commands are turned off. Contact TN support for details.

Normal Conditions Causing High CPU Load

A busy CPU is normal in some network deployments. Generally, the larger the Layer 2 or Layer 3 network, the greater the demand on the CPU to process network related traffic. Operations with the potential to cause high CPU utilization can include Spanning Tree, IP Routing table updates, encryption via the S4224 software, fragmentation causing the CPU to reassemble numerous packets, or certain CLI commands (e.g., write memory, show config).

Other events that can cause high CPU utilization may include frequent / large number of IGMP requests, the CPU generating numerous ICMP or traceroute packets, SNMP polling activities, numerous simultaneous DHCP requests (e.g., links being restored to numerous clients), ARP broadcast storms, and/or Ethernet broadcast storms.

For Additional High CPU Load TS Information

For troubleshooting High CPU Utilization in Windows see <http://technet.microsoft.com/en-us/library/bb742546.aspx>.

For troubleshooting High CPU Usage on a Domain Controller see <http://technet.microsoft.com/en-us/library/bb727054.aspx>.

For troubleshooting High CPU Utilization issues using **Tracelog** see <http://blogs.technet.com/b/askperf/archive/2012/01/20/troubleshooting-high-cpu-utilization-issues-using-tracelog-exe.aspx>.

For troubleshooting High CPU Utilization in Linux see the documentation for your particular distribution. The Linux **top** program provides a dynamic real-time view of a running system. It can display system summary information as well as a list of tasks currently being managed by the Linux kernel. The Linux CPU utilization displays CPU stats in the **CPU(s)** row and the **%CPU** column.

A task's share of the elapsed CPU time since the last screen update is expressed as a percentage of total CPU time. The top command produces a frequently-updated list of processes. By default, the processes are ordered by percentage of CPU usage, with only the "top" CPU consumers shown. Type q to exit the top command display when done. You can also install a special package called **sysstat** to take advantage of helpful commands. The **sysstat** package includes system performance tools for Linux (Red Hat Linux / RHEL includes these tools by default).

S4224 Error Recovery

The S4224 displays error and information messages from the CLI and Web interface. This section lists the messages, provides an example, and discusses the message meaning of and possible recovery steps.

As a general troubleshooting step for problems encountered using the S4224 web interface, try the related CLI command. For many messages, recovery involves reviewing the command/function description and verifying the entry selection/syntax. For example, for many CLI messages, the first recovery step would be to refer to the “S4224 CLI Reference Guide” manual.

For any error condition, you can check the [TN Tech Support web](#) site for possible solutions. For any problem that persists, contact TN Tech Support in the US or Canada at 1-800-260-1312, International at 00-1-952-941-7600; via fax at +1 952-941-2322; or via Email at techsupport@transition.com.

Generic Message Recovery (e.g., you tried a function, but the operation failed or is still in process):

1. Wait for a few moments for the operation to complete.
2. Use the **Help** or **?** command to get assistance (help) on a group of commands or on a specific command.
3. Make sure this is the function you want and that the device/port/configuration supports this function.
4. Verify the parameters entered and re-try the function. See the related section of this manual for specifics.
5. Try using the CLI to perform the function. Refer to the “S4224 CLI Reference Guide” manual.
6. If the “continue **y**(es) **n**(o) prompt” displays, type **y** and press **Enter** to continue.
7. Use the [Monitor](#) sub-menu functions (System, Ports, Link OAM, MAC Table, VLANS) to view related status, statistics, events, etc. related to a specific function.
8. Use the [Diagnostics](#) Main Menu sub-menu functions (Ping, Link OAM MIB Retrieval, VeriPHY) to test a general functionality.
9. Use the [Maintenance Menu](#) sub-menu functions (Restart the S4224, Reset the S4224 to factory defaults, Upgrade the S4224 firmware).
10. If the problem persists, contact TN Tech Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600; [TN Tech Support web](#); fax: +1 952-941-2322; Email: techsupport@transition.com.

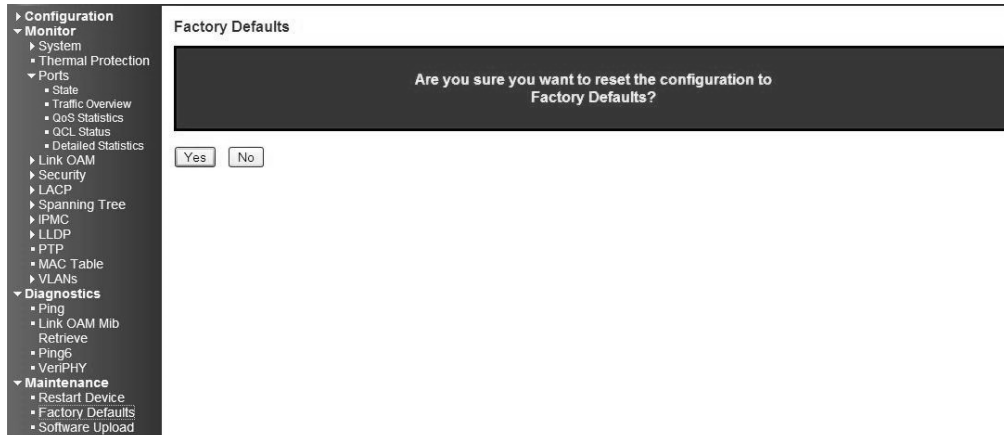
Specific Messages Recovery:

1. For messages (e.g., ACL messages) that are the result of a switch memory shortage:
 - a. Reduce other system activity to ease memory demands.
 - b. Use a less complicated configuration that requires less memory.
 - c. Modify the ACL configuration to use fewer resources, or rename the ACL with a name or number that alphanumerically precedes the other ACL names or numbers.
 - d. Reduce the number of IP or MAC access lists to be applied to interfaces.
 - e. Reduce other system activity to ease memory demands (e.g., remove ACLs that are defined but not used; use simpler ACLs with fewer ACEs; use fewer VLANs / remove unneeded VLANs from the VLAN database).
2. For messages that indicate the configuration is too complicated for the ACL code to support, there is likely too many separate access lists in a single VLAN map or policy map. Reduce the number of IP or MAC access lists separately) in any one VLAN or policy map to fewer than the number of levels. Or try to use the same ACLs on multiple interfaces if possible.
3. For messages that indicate an illegal configuration, reconfigure the port / device, removing the illegal configuration.
4. For messages that indicate the temperature is high reduce the temperature in the room.

5. For messages that indicate that the number of MAC address entries for the VLAN exceeds the maximum number allowed, have your system administrator configure an action.
6. For messages that indicate that an unauthorized device attempted to connect on a secure port, identify the device that attempted to connect on the secure port and notify your network system administrator of the condition.
7. For messages that indicate that the amount of traffic detected on the interface has exceeded the configured threshold values, determine and fix the root cause of the excessive traffic on the interface.
8. For messages that indicate an unrecoverable software error has occurred, copy the message exactly as it appears on the console or in the system log and contact TN Support.

Web Interface Messages

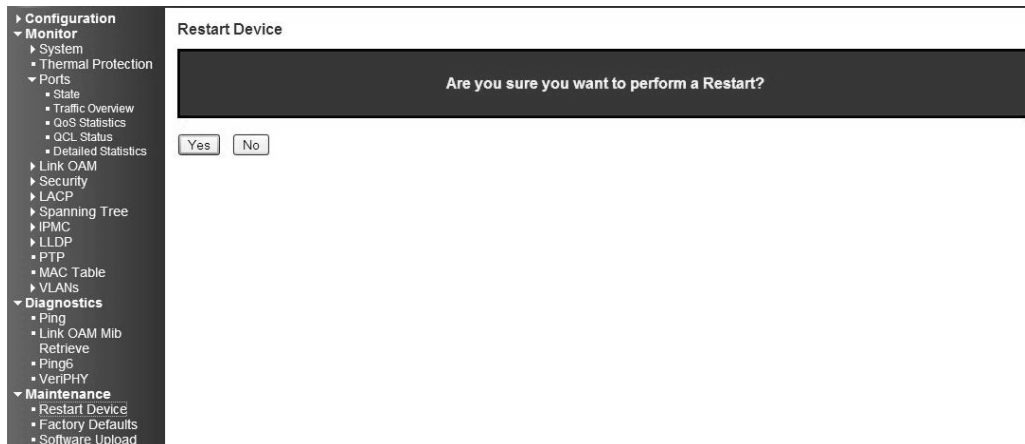
Message: Factory Defaults - Are you sure you want to reset the configuration to Factory Defaults? Yes No



Meaning: Confirmation message displayed when you select **Maintenance > Factory Defaults**.

Recovery: None; confirm that you want to reset the S4224 to its factory default settings (click **Yes**), or clear the message and continue using the current configuration (click **No**).

Message: Restart Device - Are you sure you want to perform a Restart? Yes No



Meaning: Confirmation message; you selected **Maintenance > Restart Device**.

Recovery: None; confirm that you want to restart (soft boot) the S4224 (click **Yes**), or clear the message and continue operation (click **No**).

Message: Invalid Firmware Image - The uploaded firmware image is invalid. Please use a correct firmware image.



Meaning: At **Maintenance > Software Upload** you entered or selected an unacceptable file (image).
Recovery:

1. Click the browser’s **Back** key to return to the main menu.
2. Enter or Browse to and select an acceptable file (image) from a valid location (e.g., C:\ *TFTP-Root*).
3. Click the **Upload** button. See the “Software Upload” section for more information.
4. If the problem persists, contact TN Tech Support.

Message: Invalid parameter


| Delete | Instance | Domain | Mode | Direction | Residence Port | Level | Flow Instance | Tagged VID | -----This MAC----- | Alarm |
|--------------------------|----------|--------|------|-----------|----------------|-------|---------------|------------|--------------------|----------------------------------|
| <input type="checkbox"/> | 1 | Port | Mep | Ingress | 9 | 3 | 9 | 100 | 00-01-C1-00-69-99 | <input type="radio"/> |
| <input type="checkbox"/> | 2 | Port | Mep | Ingress | 1 | 0 | 1 | 0 | 00-01-C1-00-69-91 | <input checked="" type="radio"/> |
| <input type="checkbox"/> | 3 | Port | Mep | Ingress | 1 | 0 | 1 | 0 | 00-01-C1-00-69-91 | <input checked="" type="radio"/> |

Meaning:

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Change the Instance Number or Residence Port entry.
3. See “[MEP Instance Configuration](#)” on page 217.
4. If the problem persists, contact TN Tech Support.

Message: Do you want to log out the web site?

Meaning: You clicked the Logout () button.

Recovery: Confirmation message only; click the webpage **OK** button to continue to log out of the S4224 web interface session, otherwise, click the **Cancel** button to continue working in the current S4224 web session.

If you click the **OK** button to log out, the session terminates (ends) and the Connect to screen displays:




You can log in again at any time.

Message: W_port and E_port can not be the same

Configuration > Ethernet Ring Protection Switching

| Delete | ERPS ID | Port 0 | Port 1 | Port 0 SF MEP | Port 1 SF MEP | Port 0 APS MEP | Port 1 APS MEP | Ring Type | Interconnected Node | Virtual Channel | Major Ring ID | Alarm |
|--------------------------|---------|--------|--------|---------------|---------------|----------------|----------------|-----------|--------------------------|--------------------------|---------------|--------------------------|
| <input type="checkbox"/> | 1 | 8 | 7 | 1 | 2 | 1 | 2 | Major | No | No | 1 | <input type="checkbox"/> |
| Delete | 0 | 1 | 1 | 1 | 1 | 1 | 1 | Major | <input type="checkbox"/> | <input type="checkbox"/> | 0 | <input type="checkbox"/> |

Add new Protection Group Save Reset

Message from webpage
 W_port and E_port can not be same
 OK

Meaning:**Recovery:**


1. Click the **OK** button to clear the webpage message.
2. Change the **Port 0** or the **Port 1** field so that they have different entries.
3. Click the **Save** button.
4. If the problem persists, contact TN Tech Support.

Message: West RAPS MEP and East RAPS MEP can not be the same

Configuration > Ethernet Ring Protection Switching

| Delete | ERPS ID | Port 0 | Port 1 | Port 0 SF MEP | Port 1 SF MEP | Port 0 APS MEP | Port 1 APS MEP | Ring Type | Interconnected Node | Virtual Channel | Major Ring ID | Alarm |
|--------------------------|---------|--------|--------|---------------|---------------|----------------|----------------|-----------|--------------------------|--------------------------|---------------|--------------------------|
| <input type="checkbox"/> | 1 | 8 | 7 | 1 | 2 | 1 | 2 | Major | No | No | 1 | <input type="checkbox"/> |
| Delete | 0 | 1 | 2 | 1 | 1 | 1 | 1 | Major | <input type="checkbox"/> | <input type="checkbox"/> | 0 | <input type="checkbox"/> |

Add new Protection Group Save Reset

Message from webpage
 West RAPS MEP and East RAPS MEP can not be same
 OK

Meaning: At **Configuration > ERPS** you tried to add a new Protection Group, but the operation failed when you clicked the **Save** button. Note that the number refers to the MEP instance number and not the MEP ID (which may or may not be the same).

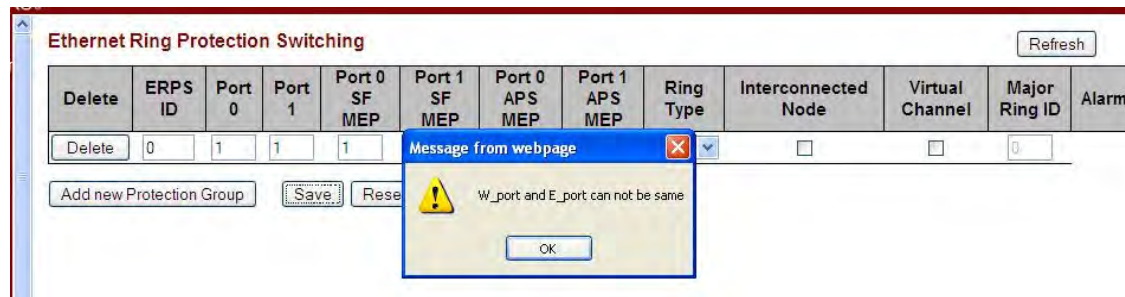
Recovery:

1. Click the **OK** button to clear the webpage message.
2. Change the **Port 0 SF MEP** or the **Port 1 SF MEP** field so that they have different entries.
3. Click the **Save** button.
4. If the problem persists, contact TN Tech Support.

Message:

West MEP and East MEP can not be the same

W_port and E_port cannot be the same

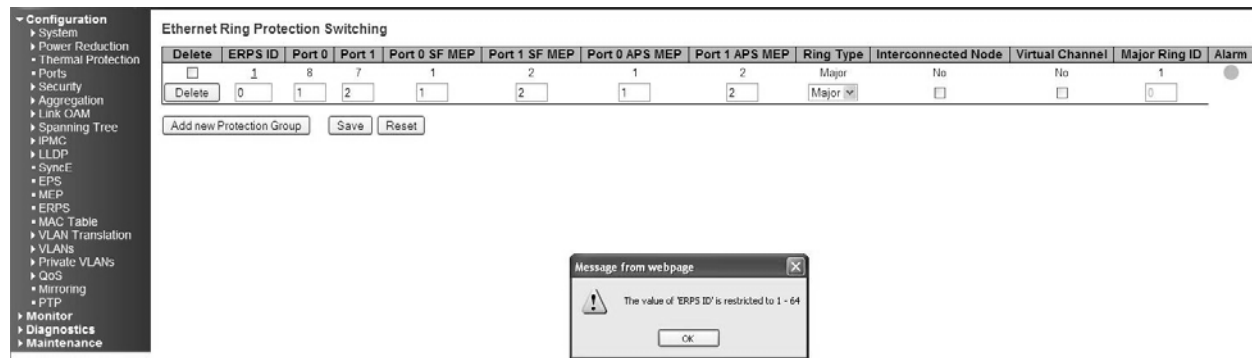


Meaning: At **Configuration > ERPS** you tried to add a new Protection Group, but the operation failed when you clicked the **Save** button.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Change the **Port 0 APS MEP** or the **Port 1 APS MEP** field so that they have different entries.
3. Click the **Save** button.
4. If the problem persists, contact TN Tech Support.

Message: **The value of ERPS ID is restricted to 1-64**

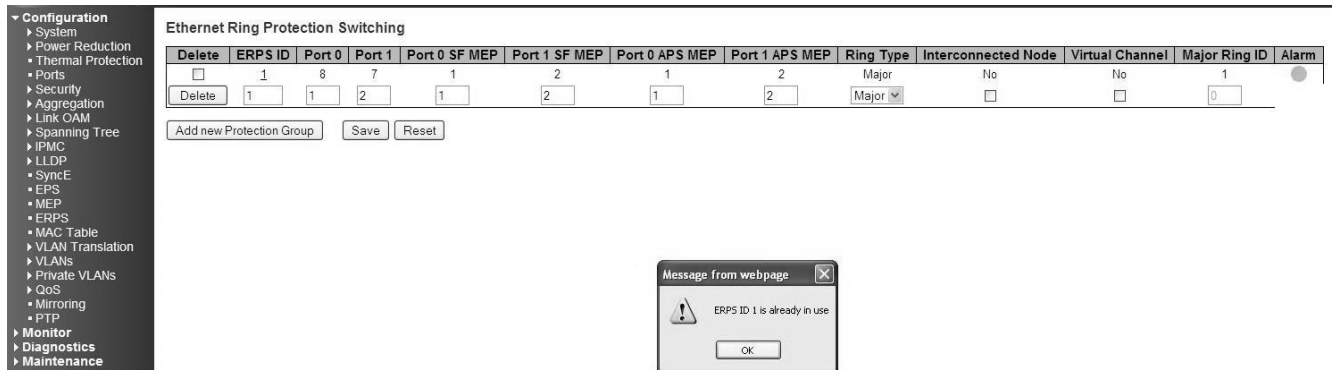


Meaning: At **Configuration > ERPS** you tried to add a new Protection Group, but the operation failed when you clicked the **Save** button.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. In the **ERPDS ID** field, enter a unique ID number of 1-64.
3. Click the **Save** button.
4. If the problem persists, contact TN Tech Support.

Message: ERPDS ID 1 is already in use

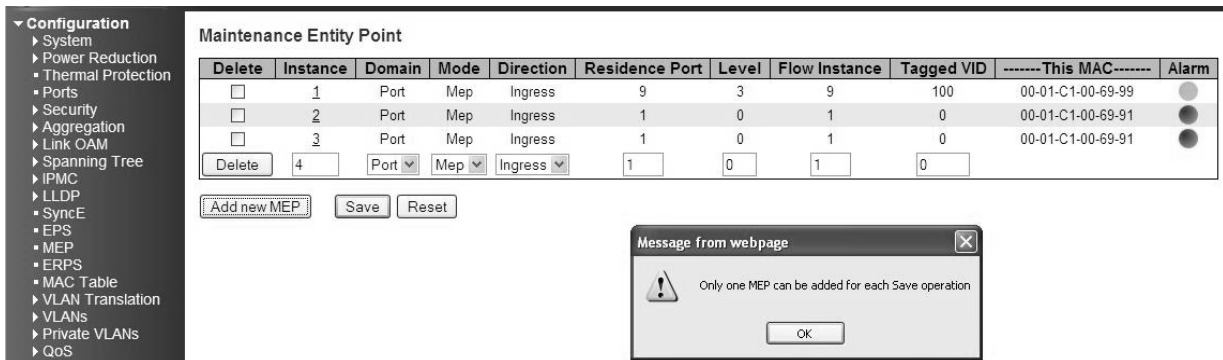


Meaning: At **Configuration > ERPS** you tried to add a new Protection Group, but the operation failed when you clicked the **Save** button.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. In the **ERPDS ID** field, enter a unique ID number of 1-64.
3. Click the **Save** button.
4. If the problem persists, contact TN Tech Support.

Message: Only one MEP can be added for each Save operation



Meaning: At **Configuration > MEP** you clicked **Add New MEP** before you saved the MEP you were already adding.

Recovery:

1. Click **OK** to clear the webpage message.
2. Click the **Save** button, and make the required MEP config selections.
3. Click the **Add a new MEP** button to configure the next new MEP.
4. If the problem persists, contact TN Tech Support.

Message: Invalid parameter

Example:

Maintenance Entity Point

| Delete | Instance | Domain | Mode | Direction | Residence Port | Level | Flow Instance | Tagged VID | -----This MAC----- | Alarm |
|--------------------------|----------|--------|------|-----------|----------------|-------|---------------|------------|--------------------|----------------------------------|
| <input type="checkbox"/> | 1 | Port | Mep | Ingress | 9 | 3 | 9 | 100 | 00-01-C1-00-69-99 | <input type="radio"/> |
| <input type="checkbox"/> | 2 | Port | Mep | Ingress | 1 | 0 | 1 | 0 | 00-01-C1-00-69-91 | <input checked="" type="radio"/> |
| <input type="checkbox"/> | 3 | Port | Mep | Ingress | 1 | 0 | 1 | 0 | 00-01-C1-00-69-91 | <input checked="" type="radio"/> |
| <input type="checkbox"/> | 4 | Port | Mep | Ingress | 1 | 0 | 1 | 0 | 00-01-C1-00-69-91 | <input checked="" type="radio"/> |
| <input type="checkbox"/> | 5 | Port | Mep | Ingress | 1 | 0 | 1 | 0 | 00-01-C1-00-69-91 | <input checked="" type="radio"/> |

Buttons: Add new MEP, Save, Reset

Message from webpage: Invalid parameter (OK)

Meaning: At **Configuration > MEP > Add New MEP** you selected an unsupported feature (e.g., Mode = MIP).

Recovery:

1. Click **OK** to clear the webpage message.
2. Click the **Add a new MEP** button, make another (valid / supported) selection, and then click **Save**.
3. If the problem persists, contact TN Tech Support.

Message: Group ID 3 and VID: 4 combination is already in use. Please update existing entry instead of adding it again!

Example:

VLAN Translation Table

| Delete | Group ID | VLAN ID | Translated to VID |
|--------|----------|---------|-------------------|
| Delete | 1 | 2 | 3 |
| Delete | 2 | 3 | 4 |
| Delete | 3 | 4 | 5 |
| Delete | 3 | 4 | |

Buttons: Add new entry, Save, Reset

Auto-refresh Refresh

Message from webpage: Group ID 3 and VID: 4 combination is already in use. Please update existing entry instead of adding it again! (OK)

Meaning: At **VLAN Translation > VID Translation Mapping**, you tried to enter duplicate information.

Recovery:

1. Make sure the **Group ID**, **VLAN ID**, and **Translated to VID** entries are unique (do not already exist in the VLAN Translation Table).
2. Continue the operation.
3. If the problem persists, contact TN Tech Support.

Message: Group ID field cannot be empty. Please check help page for correct Group ID format.

Example:

The screenshot shows the 'VLAN Translation Table' configuration page. A table with columns 'Delete', 'Group ID', 'VLAN ID', and 'Translated to VID' is visible. Below the table are buttons for 'Delete', 'Add new entry', 'Save', and 'Reset'. An error message dialog box is displayed in the foreground, stating: 'Group ID field can not be empty. Please check help page for correct Group ID format.' The dialog has an 'OK' button.

Meaning:

At **VLAN Translation > VID Translation Mapping**, you tried to Add a new entry, but did not enter a Group ID.

Recovery:

1. Make sure the **Group ID**, **VLAN ID**, and **Translated to VID** entries are made in the VLAN Translation Table).
2. Continue the operation.
3. If the problem persists, contact TN Tech Support.

Message: Deleting all VLANs will cause loss of connection to the switch. Continue?

Example:

The screenshot shows the 'VLAN Membership Configuration' page. It includes a table with columns 'Delete', 'VLAN ID', 'VLAN Name', and 'Port Members' (sub-columns 1-8). The first row shows VLAN ID 1, named 'default', with all port members checked. A warning dialog box is displayed, asking: 'Deleting all VLANs will cause loss of connection to the switch. Continue?' with 'OK' and 'Cancel' buttons.

Meaning: At **Configuration > VLANs > VLAN Membership**, you tried to delete VLAN ID 1 from the 'VLAN Membership' table. This is the default VLAN; if you delete it the S4224 connection will drop.

Meaning: You tried to delete a non-existent VLAN translation entry from a group.

Recovery:

1. Make sure this is the action you want. If so, click the **OK** button; if not, click the **Cancel** button to clear the webpage message. Continue operation.
2. Re-enter the command with a different (existing) group.
3. Add port member to the group and re-try the operation.
4. Make sure you are not trying to delete VLAN 1. Deleting VLAN 1 causes issues with forwarding.
5. To make sure no ports belong to VLAN 1, add VLAN 1 with all ports in the forbidden state.
6. See the **Delete VLAN Translation Group Entry** command for CLI information.
7. If a problem persists, contact TN Tech Support.

Message: The value of ‘Queue Shaper Rate’ is restricted to 100 - 1000000 kbps. Select the ‘Mbps’ unit for coarser granularity.

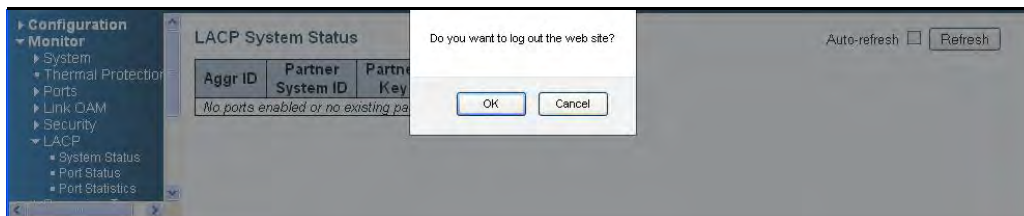


Meaning: At **Configuration > QoS > Port Scheduler**, you selected too high or low a number for the unit of measure. You selected too fine of a granularity (measurement). The shaper granularity is in steps of 400Kbps, so for low rates like 600Kbps you cannot hit exactly this rate. The shaper can be set in steps of 100Kbps, but is only accurate at 400Kbps boundaries. The Shaper works accurately at 400Kbps increments, but anything less yields an inaccurate result.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Select another unit of measure (‘kbps’ or ‘mbps’) and continue operation.
3. If a problem persists, contact TN Tech Support.

Message: Do you want to log out the web site?



Meaning: FireFox message that displays when you click the web interface **Logout** button.

Recovery:

1. Click the **OK** button to clear the webpage message. The login prompt displays again.
2. Continue operation - if desired, log back in to the S4224 web interface.
3. If a problem persists, contact TN Tech Support.

**Message: The value of Port Error Recovery Timeout is 30-84600
The value of Port Error Recovery Timeout cannot be empty**



Meaning: At **Configuration > Spanning Tree > Bridge Settings** you entered an invalid value in the “Port Error Recovery Timeout” field.

Recovery:

1. Enter a value in the range of 30-84,600 seconds (½ minute - 1243.3 minutes or 20.72 hours).
2. Continue operation.
3. If a problem persists, contact TN Tech Support.

Message: OAM Error - Invalid request on this port

Example:



Meaning:

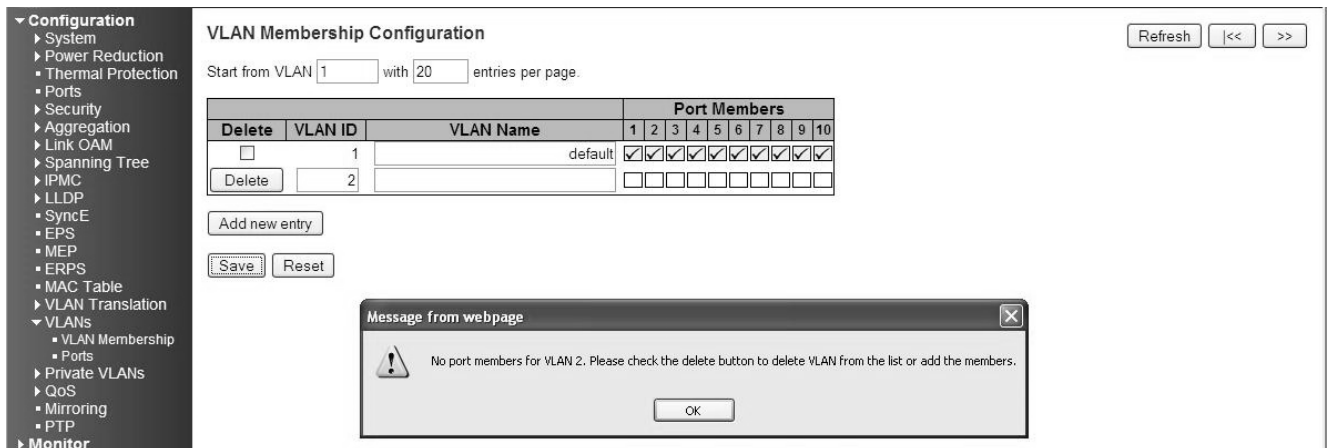
At **Diagnostics > Link OAM Mib Retrieve** you selected a port that is not ...

Recovery:

1. Click the browser's back button to clear the message, verify your selection. .
2. Make sure you have selected either the "Local" or "Peer" radio button.
3. Verify the port number selected.
4. If a problem persists, contact TN Tech Support.

Message: No port members for VLAN x. Please check the delete button to delete the VLAN from the list or add the members.

Example:



Meaning: At **Configuration > VLANs > VLAN Membership** you tried to add a VLAN to the VLAN membership configuration, but you did not check any of the Port Members checkboxes. Note: VLAN 1 cannot be deleted.

Recovery:

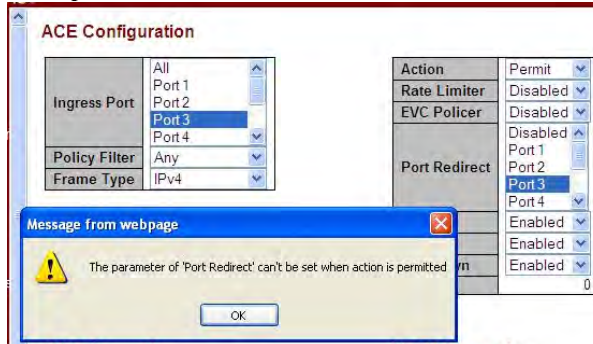
1. Click the **OK** button to clear the webpage message.
2. Either a) click the **Delete** button to delete the VLAN from the list, or b) click one or more Port Members checkboxes in the table and click the **Save** button to add the new entry.
3. If a problem persists, contact TN Tech Support.

Message: The parameter of 'port_copy' can't be set when action is permitted

Meaning: At **Configuration > Security > Network > ACL > Ports** you set the “Action” parameter to “Permit”, which does not allow the “Port Copy” parameter to be set to a Port (**Port 3** on the screen above).

Recovery:

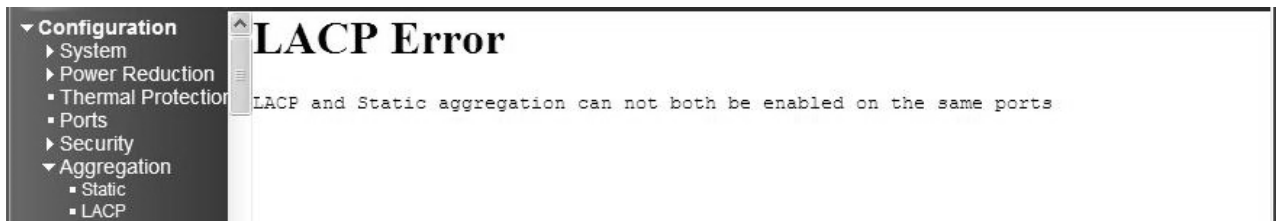
1. Click the **OK** button to close the webpage message.
2. Either a) change the “Action” parameter selection, or b) change the “Port Copy” parameter selection to “Disabled”.
3. Click the **Save** button when done.
4. If a problem persists, contact TN Tech Support.

Message: The parameter of 'Port Redirect' can't be set when action is permitted**Example:**

Meaning: At **Configuration > Security > Network > ACL > Access Control List** you set the “Action” parameter to “Permit”, which does not allow the “Port Redirect” parameter to be set to a Port (**Port 3** on the screen above).

Recovery:

1. Click the **OK** button to close the webpage message.
2. Either a) change the “Action” parameter selection, or b) change the “Port Redirect” parameter selection to “Disabled”.
3. Click the **Save** button when done.
4. If a problem persists, contact TN Tech Support.

Message: Aggregation Error - Port joining aggregation must be in the same speed and in full duplex Group 1 member counts error!! Local aggregation must include 2-16 ports.**LACP Error - LACP and Static aggregation can not both be enabled on the same ports****Example:**

Meaning: You configured a port for both LACP and Static aggregation, which is not supported. For example, at **Configuration > Aggregation > Static**. and at **Configuration > Aggregation > LACP** you configured a port for both LACP and Static aggregation, which is not supported.

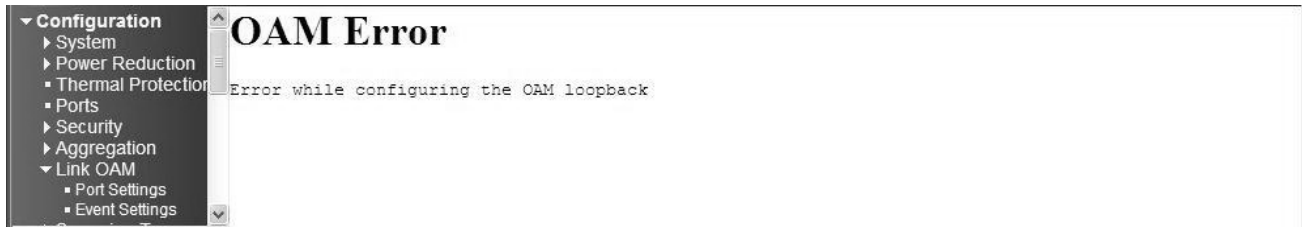
Recovery:

1. Click the browser ‘Back’ button to clear the message.

2. Make sure each port has one configuration (either LACP or Static aggregation) enabled.
3. Verify the aggregation path configuration, click Save, and continue operation. See the “[Aggregation Configuration](#)” section on page 63.
4. If a problem persists, contact TN Tech Support.

Message: OAM Error - Error while configuring the OAM loopback

Example:



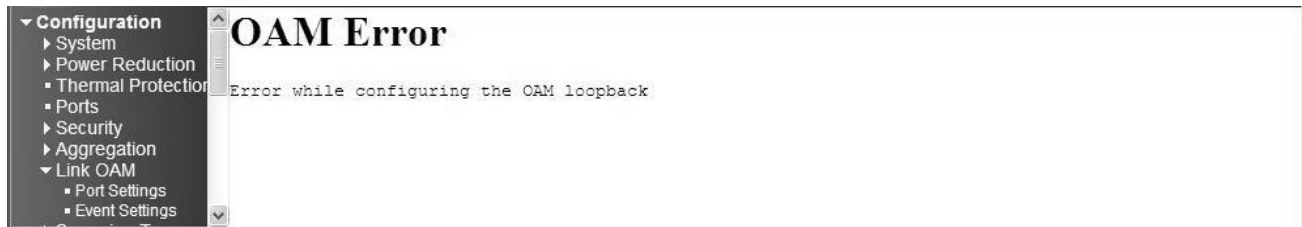
Meaning: At **Configuration > Link OAM > Port Settings** you entered an invalid parameter.

Recovery:

1. Click the browser ‘Back’ button to clear the message.
2. Make sure the Loopback Operation checkbox is unchecked.
3. Verify the ‘Link OAM Port Configuration’ table selections, click **Save**, and continue operation. See the “[Link OAM \(LOAM\) Configuration](#)” section on page 148.
4. If a problem persists, contact TN Tech Support.

Message: OAM Error - Error While Configuring Link Events

Example:



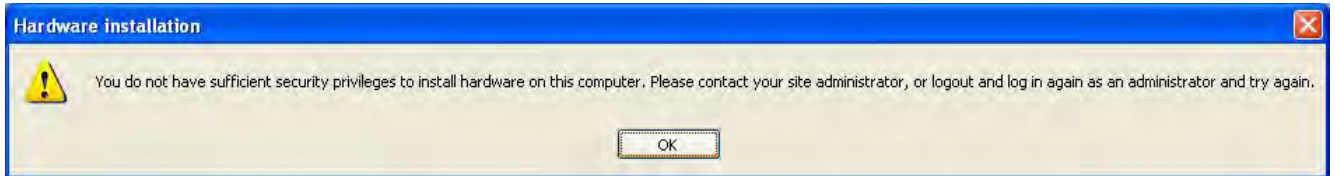
Meaning: At **Configuration > Link OAM > Event Settings** you entered an invalid parameter.

Recovery:

1. Click the browser ‘Back’ button to clear the message.
2. Verify the ‘Link Event Configuration for Port x’ selections, click ‘**Save**’, and continue operation.
3. If a problem persists, contact TN Tech Support.

Message: HW Install - cannot start with this user account. Make sure this user account is a member of the Administrators group on this computer.

You do not have sufficient security privileges to install hardware on this computer. Please contact your site administrator, or logout and log in again as an administrator and try again.

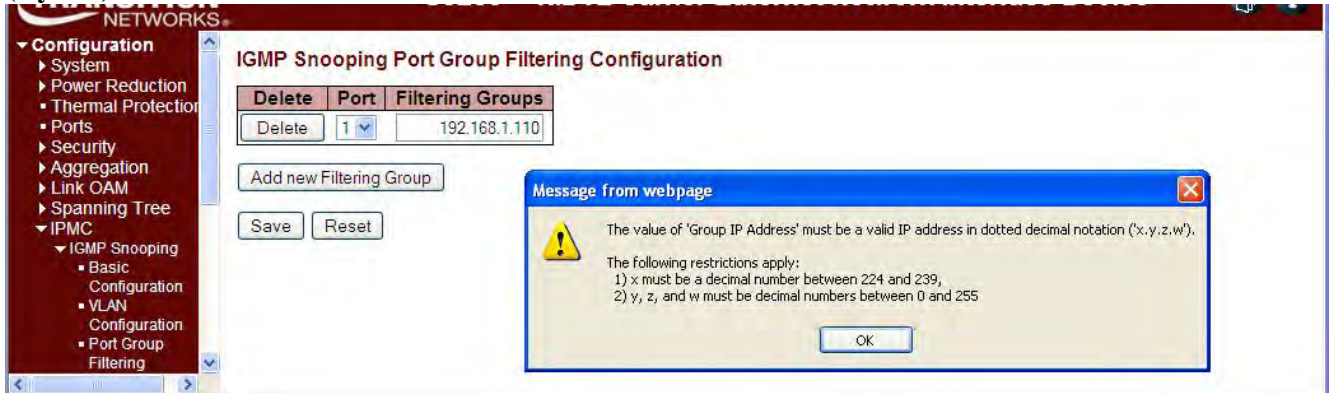


Meaning: A privilege level issue exists.

Recovery:

1. Contact your system administrator, or change your user privilege to Admin.
2. Click the **OK** button to clear the message.
3. Continue operation.
4. If a problem persists, contact TN Tech Support.

Message: The value of 'Group IP Address' must be a valid IP address in dotted decimal notation (x.y.z.w).

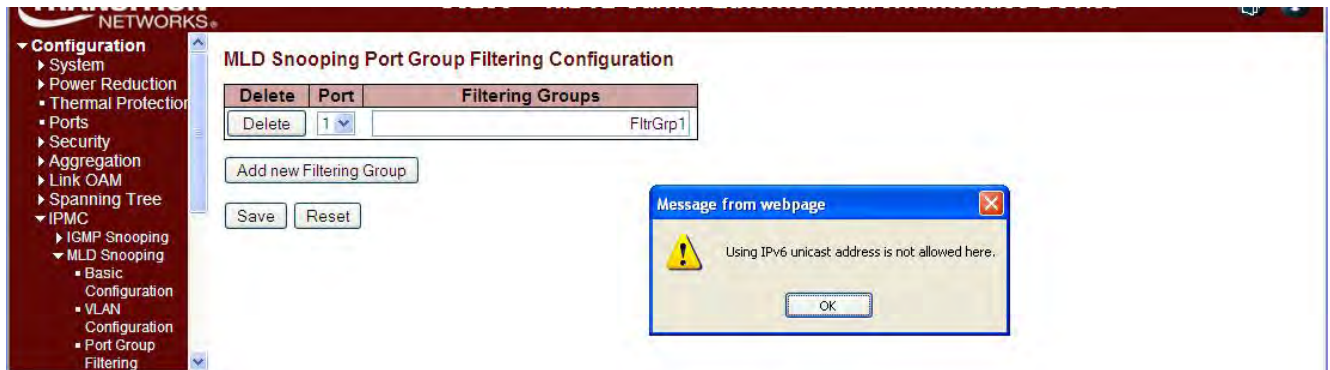


Meaning: At **Configuration > IPMC > IGMP Snooping > Port Group Filtering**, you entered an invalid IP address.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Make sure the IP Address you enter is in dotted decimal notation (x.y.z.w), where:
 - x is a decimal number from 224 to 239, and
 - y, z, and w are decimal numbers from 0 to 255.
3. Continue operation. See the “[Port Group Filtering](#)” section on page 100.
4. If a problem persists, contact TN Tech Support.

Message: Using IPv6 unicast address is not allowed here.



Meaning: At **Configuration > IPMC > MLD Snooping > Port Group Filtering** you entered an IPv6 unicast address in the Filtering Groups field.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Make sure the IP Address you enter is an IPv6 multicast address.
3. Continue operation. See the “[Port Group Filtering](#)” section on page 100.
4. If a problem persists, contact TN Tech Support.

Message: The value of ‘Group Address’ must be a valid IPv6 address in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:).

Meaning: At **Configuration > IPMC > MLD Snooping > Port Group Filtering** you entered an invalid IP address in the Filtering Groups table / field.



Meaning: At **Configuration > IPMC > MLD Snooping > Port Group Filtering** you entered an IPv6 unicast address in the Filtering Groups field.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Make sure the IP Address you enter is a valid IPv6 address in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:).
3. Continue operation. See the “[Port Group Filtering](#)” section on page 100.
4. If a problem persists, contact TN Tech Support.

Message:

Entry with Group ID: x already exists, Please give other Group ID value.

Invalid Group ID value: xx. Group ID must be an integer between 1 to 8.

The maximum entries possible is 6

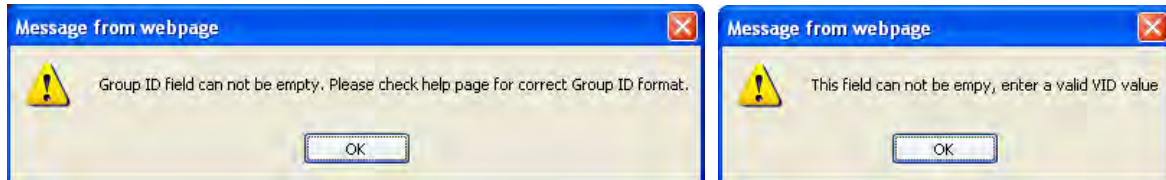
Meaning: At **Configuration > VLAN Translation** you entered a Group ID number outside of the valid range of 1-8, or you entered an existing Group ID number.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Enter a valid, unique Group ID number and click the **Save** button. See “[Port to Group Mapping](#)” on page 131.
3. Verify that the Add New Entry was successful, and continue operation.
4. If a problem persists, contact TN Tech Support.

Message: **This field can not be empty, enter a valid VID value.**

Example: Group ID field can not be empty. Please check help page for correct Group ID format.



Meaning:

Recovery: At **Configuration > VLAN > VLAN Membership** you did not enter a Group ID or VLAN ID.

1. Click the **OK** button to clear the webpage message.
2. Enter a valid, unique Group ID number or VLAN ID number and click the **Save** button. See “[IP Configuration](#)” on page 18.
3. Verify that the entry was successful, and continue operation.
4. If a problem persists, contact TN Tech Support.

Message: **Collecting initial data, please wait ..**

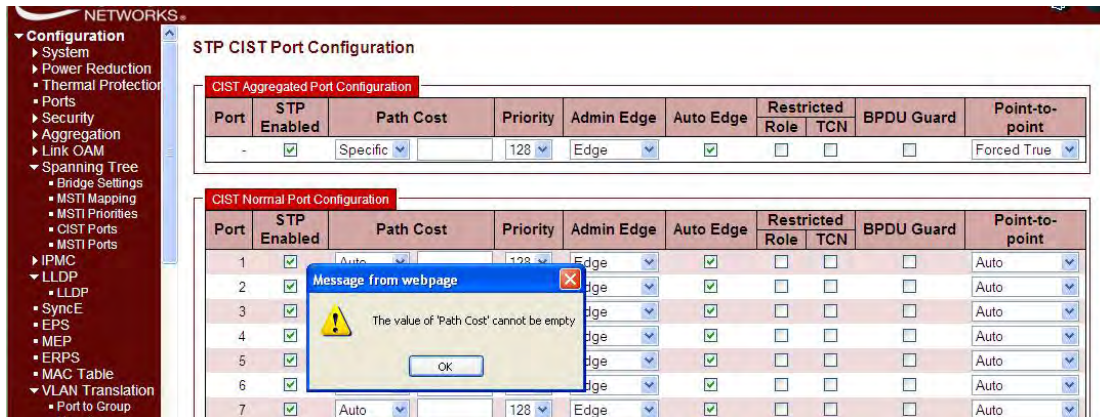


Meaning: Displayed in Google Chrome or Mozilla Firefox at the **Monitor > System > CPU Load** menu path. This page displays the CPU load, using an SVG graph. In order to display the SVG graph, your browser must support the SVG format.

Recovery:

1. See the SVG Wiki at http://wiki.svg.org/index.php/Viewer_Implementations for more information on browser support.
2. At the [SVG Wiki](#), check for native implementations and/or download available Browser Plug-Ins.
3. Retry the operation. If necessary, use Internet Explorer as your web browser.
4. If a problem persists, contact TN Tech Support.

**Message: The value of Path Cost cannot be empty
The value of 'Path Cost' is restricted to 1 - 200000000**

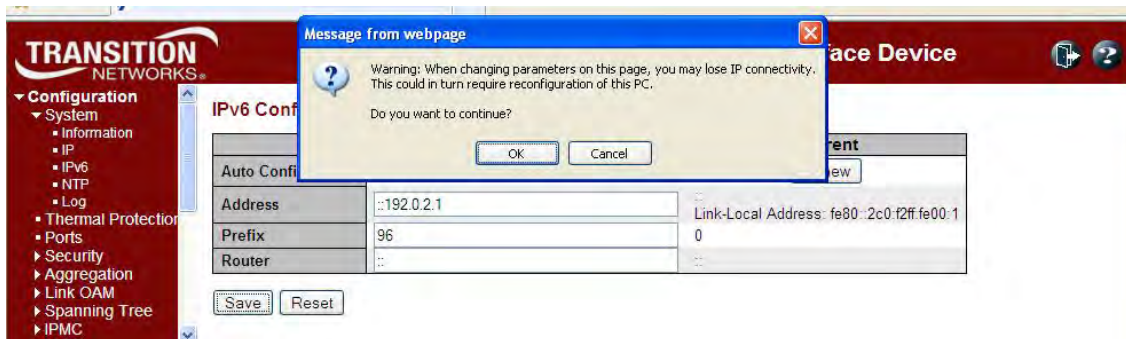


Meaning: At **Configuration > Spanning Tree > CIST Ports** you selected “**Specific**” in the **Path Cost** dropdown, but did not enter a value in the **Path Cost** entry field.

Recovery:

1. Click **OK** to clear the webpage message.
2. Either enter a valid **Path Cost** (1 - 200,000,000) in the entry field, or select **Auto** at the dropdown. See “**CIST Ports**” on page 164.
3. If a problem persists, contact TN Tech Support.

Message: Warning: When changing parameters on this page, you may lose IP connectivity. This could in turn require reconfiguration of this PC. Do you want to continue?

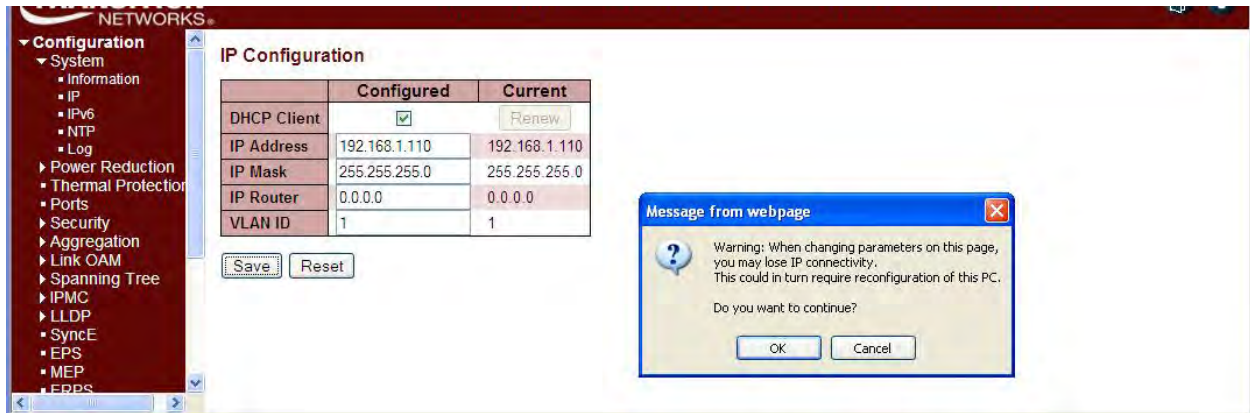


Meaning: At **Configuration > System > IPv6** you checked the **Auto Configuration** checkbox and clicked **Save**.

Recovery:

1. Verify that this is the function that you want to perform and be aware of the consequences mentioned.
2. Determine whether your particular computer will require reconfiguration. For example, for Microsoft .NET Framework version 2.0 and later, IPv6 is enabled by default. For .NET Framework version 1.1 and earlier, IPv6 is disabled by default. For more information see the MSDN article at <http://msdn.microsoft.com/en-us/library/8db2058t.aspx>. Windows Server 2008 provides complete support for IPv6 and all of its features, and does not need additional installation or configuration. For Windows 7 see <http://technet.microsoft.com/en-us/magazine/2009.07.cableguy.aspx>. For Windows XP see <http://support.microsoft.com/kb/2478747>. For Linux / BSD, see <http://ipv6.com/articles/applications/Linux-and-BSD.htm> or your distribution documentation and/or website.
3. Click the **OK** button only if you are sure you want to continue IPv6 Auto Configuration. Otherwise click the **No** button and click **Reset**.

Message: Warning: When changing parameters on this page, you may lose IP connectivity. This could in turn require reconfiguration of this PC. Do you want to continue?

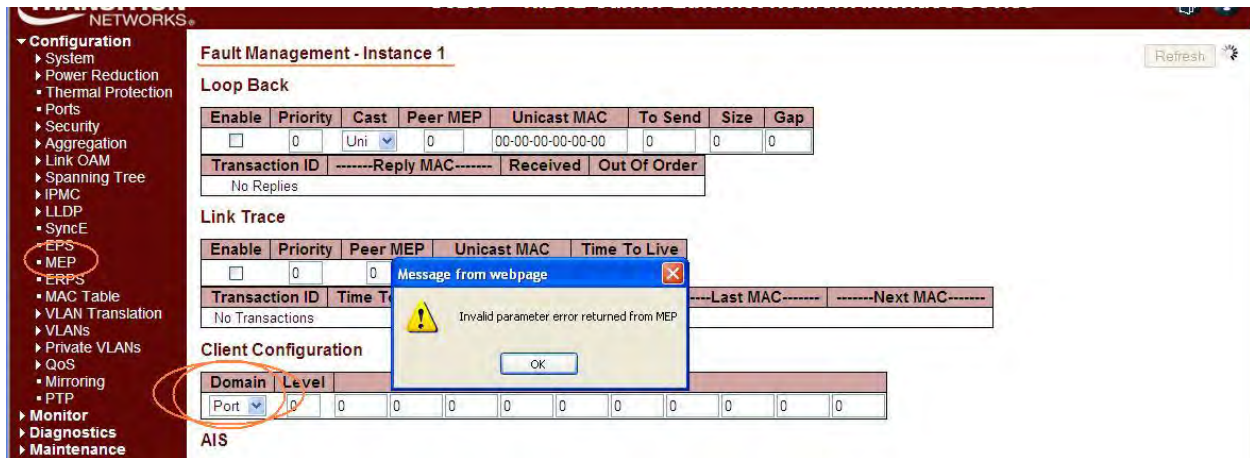


Meaning: At **Configuration > System > IP** you checked the **DHCP Client Configured** checkbox and clicked **Save**.

Recovery:

1. Verify that this is the function that you want to perform and be aware of the consequences mentioned.
2. Click the **OK** button only if you are sure you want to continue IPv6 Auto Configuration. Otherwise click the **No** button and then click **Reset**.
3. See “[IP Configuration](#)” on page 18 for more information.

Message: Invalid parameter error returned from MEP

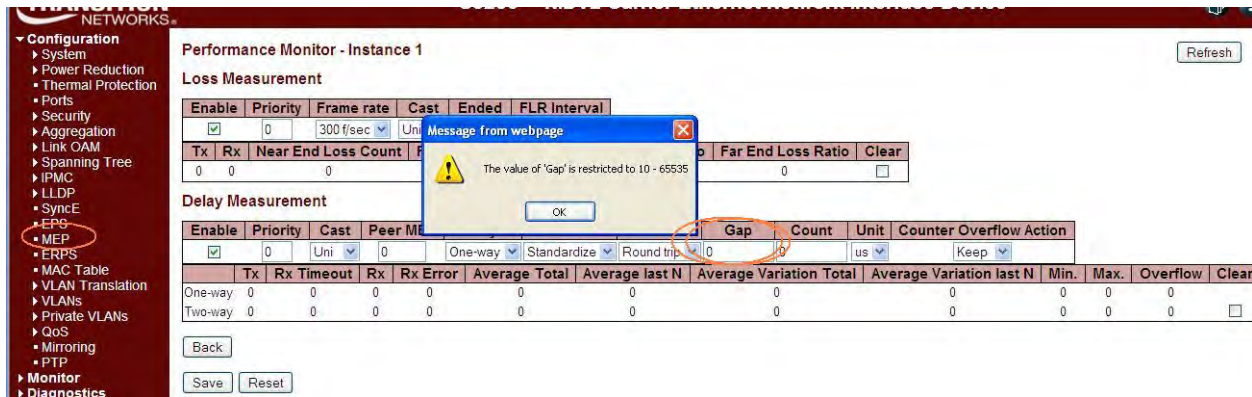


Meaning: At **Configuration > MEP > MEP Configuration > Fault Management - Instance** in the **Client Configuration** section at the **Domain** dropdown, you selected a currently unsupported client layer domain.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Select 'EVC'. Only a 'Port' MEP is able to be a server MEP having relation to a client layer. Any other selections (Esp, Evc, Mpls) are for future use.
3. See ‘[MEP Configuration](#)’ on page 213.

Message: The value of ‘Gap’ is restricted to 10-65535



Meaning: At **Configuration > MEP > Performance Monitor - Instance** in the **Delay Measurement** section in the **Gap** field, you entered an invalid value.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Enter a Gap value of 10-65535.
3. See ‘[MEP Configuration](#)’ on page 213.

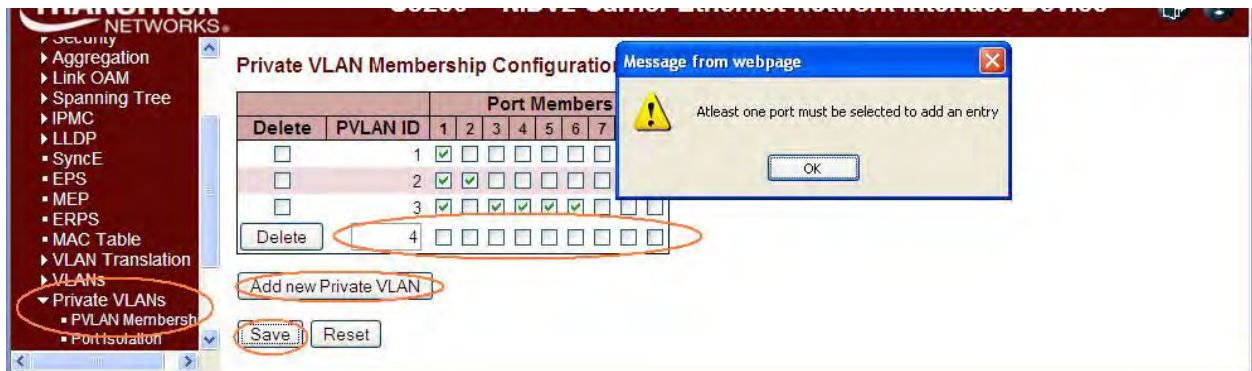
Message: The value of “Count’ is restricted to 10-2000

Meaning: At **Configuration > MEP > Performance Monitor - Instance** in the **Delay Measurement** section in the **Count** field, you entered an invalid value.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Enter a Gap value of 10-2000.
3. See ‘[MEP Configuration](#)’ on page 213.

Message: At least one port must be selected to add an entry
At least one port must be selected. To delete entry, check the delete checkbox.

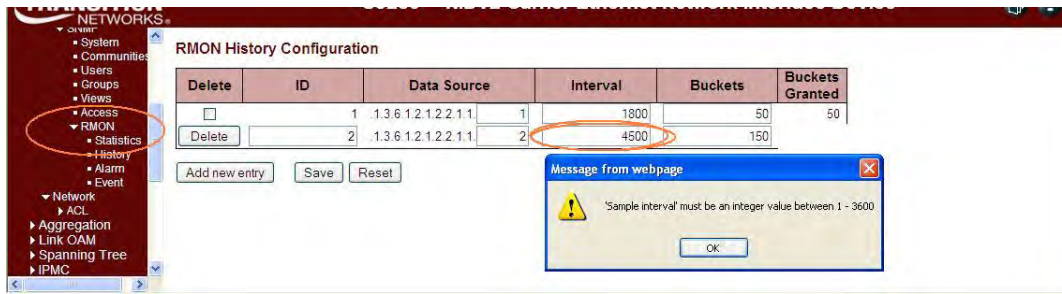


Meaning: At **Configuration > Private VLANs > PVLAN Membership** you clicked the **Save** button without first checking at least one of the **Port Membership** checkboxes.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Check one or more of the **Port Membership** checkboxes.
3. See ‘[PVLAN Membership](#)’ on page 274.

Message: ‘Sample interval’ must be an integer value between 1- 3600



Meaning: At the **Configuration > Security > Switch > SNMP > RMON > History** menu path in the **Interval** field, you entered an invalid number.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Enter a valid Interval in the range of 1 to 3600.
3. See “[Configuration > Security > Switch > SNMP > RMON](#)” on page 83.

Message: ‘Variable value’ is xxx.yyy’, xxx is 10-21, yyy is 1-65535



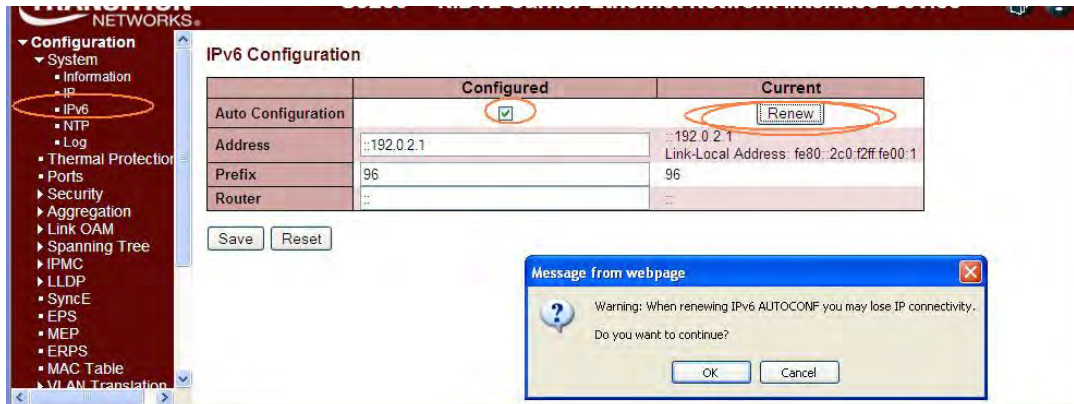
Meaning: At the **Configuration > Security > Switch > SNMP > RMON > Alarm** menu path in the **Variable** field, you entered an invalid number.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Enter a valid Variable value.
3. See “[Configuration > Security > Switch > SNMP > RMON](#)” on page 83.

Message: Warning - When renewing IPv6 AUTOCONF you may lose IP connectivity.

Example:



Meaning: At the **Configuration > System > IPv6** menu path you checked the Auto Configuration “Configured” checkbox, and then clicked the “Renew” button.

Recovery:

1. Click the **Cancel** button if you are not sure you want to renew the IPv6 Auto Configuration. Click the **OK** button only if you are sure you want to renew the IPv6 Auto Configuration, and understand that the current S4224 web session may drop.
2. See “IP Configuration” on page 22.

Message: The format of ‘Server Address’ is invalid. It must be a valid IP in dotted decimal notation ‘x.y.z.w’).

Example:



Meaning:

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Re-enter a valid IP address in dotted decimal notation (e.g., 192.168.1.30).
3. See “NTP Configuration” on page 50.

Message: This browser doesn't support dynamic tables.

Meaning: The browser you are using is not supported.

Recovery: Use a browser that the S4224 supports. See “Web Browser Support” on page 32.

Message: Port %lu does not support this mode\n

Meaning: The DMI function is not supported on this port.

Recovery:

1. Switch to another port that supports DMI.
2. Use another S4224 function.
3. See “DMI Configuration” on page 50.

Message: Can not enable HTTPS redirect function when the HTTPS operation mode is disabled.

Meaning: At **Configuration > Security > Switch > HTTPS** you selected an HTTPS configuration of Mode = Disabled and Automatic Redirect = Enabled, which is not supported.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. At **Configuration > Security > Switch > HTTPS** select an HTTPS configuration of either:
 - Mode** = Disabled and **Automatic Redirect** = Disabled, or
 - Mode** = Enabled and **Automatic Redirect** = Disabled, or
 - Mode** = Enabled and **Automatic Redirect** = Enabled.
3. See “[HTTPS Configuration](#)” on page 200 for more information.

Message: VLAN Translation Table -- Updating...

Meaning: At **Configuration > VLAN Translation > VID Translation Mapping** you tried to add a new VLAN translation table entry, but the attempt failed.

Recovery:

1. Press the **Reset** button.
2. Click the browser Back button.
3. At the CLI, enter the command **config default keep_ip** and press **Enter**.
4. Restart the S4224 web interface.

Message: The value of 'Key cannot be empty

Meaning: At **Configuration > Aggregation > LACP** you clicked the **Save** button without first entering a **Key** entry field entry.

Recovery:

1. Click the **OK** button to close the message dialog box.
2. Enter a **Key** entry field entry.
3. Click the **Save** button when done. See ‘[LACP \(Link Aggregation Control Protocol\)](#)’ on page 145.

Message: Switch does not respond.

Meaning: You tried to enable both ACL policer and EVC policer functions at the same time.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Log back in to the S4224 web interface if your web browser can no longer display the webpage.
3. Retry the operation.
4. Check the CLI for the message “*Error: ACL policer and EVC policer can not both be enabled*”.
5. At the CLI, press the **Enter** key to re-display the CLI main (startup) screen.
6. Enter the CLI command “**config default keep_config**”.
7. Log in again via the S4224 web interface.

Message: HTTPS Certificate Load Error. SSL Certificate PEM file size too big

Meaning: At **Configuration > Security > Switch > HTTPS** you tried to download a HTTPS / SSL certificate file that exceeded the file size limit.

Recovery:

1. Click the browser Back button.
2. Check the SSL certificate file in terms of size and content.
3. Retry the operation. See “[HTTPS Configuration](#)” on page 61.

Message: **The format of OID Subtree is .OID1.OID2.OID3. The allowed length is 1 to 128. The allowed string content is digital number or asterisk (*).**

Meaning: At **Configuration > Security > Switch > SNMP > Views** you entered an invalid OID Subtree value.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Enter an OID Subtree value in the correct format, length and content.
3. See “[SNMP Configuration](#)” on page 74.

Message: **‘Variable value is xxx.yyy’, xxx is 10-21, yyy is 1-65535**

Meaning: At **Config > System > Security > RMON > Alarm** you entered an invalid value.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Enter a Variable value in the correct format, length and/or content.
3. See “[SNMP Configuration](#)” on page 74.

Messages: **The HTTPS function enabled on this device. Redirect for using HTTPS ...**

Content was blocked because it was not signed by a valid security certificate.

To help protect your security, Internet Explorer has blocked this website with security certificate errors. Click here for option.

Meaning: Web browser certificate message.

Recovery:

1. Click the browser’s Back button to clear the error message.
2. See “Certificate Errors” in IE Help.
3. Click the Information Bar (“*To help protect ...*”) and then click “**Display Blocked Content**”.
4. At the message “There is a problem with this website's security certificate.”, click “*Continue to this website (not recommended).*”
5. Log back in to the S4224 system.
6. Click on ‘Certificate Error’.
7. Click on “View Certificates”.
8. Click on ‘Install Certificate...’.
9. At the “Welcome to Certificate Import Wizard” - “Welcome” screen, click **Next**.
10. At the Certificate Store” dialog box, click **Next**.
11. At the “Completing the Certificate Import Wizard” dialog box, click the “**Finish**” button. The “Security Warning” dialog box displays.
12. Click the **Yes** button.
13. When the “*Import was successful*” message displays, click the **OK** button.
14. At the Certificate dialog box / General tab, click the **OK** button.
15. Continue the operation; see “[HTTPS Configuration](#)”.

Message: HTTPS Certificate Load Error - Please disable HTTPS mode first

Meaning: At **Configuration > Security > Switch > HTTPS** you tried to load an HTTPS certificate with HTTPS mode enabled.

Recovery:

1. Click the browser Back button to clear the error message.
2. At **Configuration > Security > Switch > HTTPS** set HTTPS mode to disabled.
3. Continue the operation; see “[HTTPS Configuration](#)”.

Message: The Voice VLAN ID should not equal switch management VLAN ID

Meaning: You entered the same VLAN ID at **Configuration > MVR** and at **Configuration > Voice VLAN**.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Change the VLAN ID at MVR or at Voice VLAN. See the related section of this manual.

Message: All EVCs statistics will be cleared. Do you want to proceed anyway?

Meaning: Confirmation message. You clicked the **Clear** button at **Monitor > Ethernet Services > EVC Statistics**.

Recovery:

1. Click the **OK** button to clear the webpage message and clear all of the stored EVC statistics, or click the **Cancel** button to leave the stored EVC statistics and continue operation.
2. See “[Monitor > Ethernet Services](#)” on page 488.

Message: All EVCs statistics will be removed. Do you want to proceed anyway?

Meaning: You deleted the ECE from **Configuration > Ethernet Services > ECE**, or you checked all of the UNI Ports checkboxes in the “ECE Configuration” section.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Click the **Remove All** button. Internet connectivity is likely lost, and the S4224 web interface is temporarily unavailable.
3. From the CLI, enter the command **conf default keep_ip** and press Enter.
4. Open a new web browser session and log back in to the S4224.

Message: Frame Type: 1 and value: 0800 is already mapped to Group ID: 'a1'

Meaning: At **Configuration > VCL > Protocol-based VLAN > Protocol to Group** you tried to **Save** a second similar configuration.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Change the new entry's Frame Type and/or Value.
3. See "[Protocol-based VLAN](#)" on page 279.

Message: Port Security Error - The 802.1X Admin State must be set to Authorized for ports that are enabled for LACP

Port Security Error - The 802.1X Admin State must be set to Authorized for ports that are enabled for Spanning Tree.

Meaning: At **Security > Network > NAS** you entered an unsupported configuration and clicked the **Save** button. In the 'Port Configuration' table in the 'Admin State' column, the parameter you selected (e.g., "Port-based 802.1X") requires a configuration change before you can perform this action.

Recovery:

1. Click the browser's **Back** button to clear the message.
2. Make the requested configuration change (e.g., disable LACP for the port, or disable Spanning Tree for the port). To configure the Spanning Tree function, see **Configuration > Spanning Tree > CIST Ports > CIST Normal Port Configuration** in the "STP Enabled" column.
3. Re-try the configuration at **Security > Network > NAS**. See [Configuration > Security > Network > NAS](#) for more information.

Message:

The value of 'add group address' must be a valid IP address in dotted decimal notation ('x.y.z.w').

The value of 'Start group Address' must be a valid IP address in dotted decimal notation ('x.y.z.w').

The following restrictions apply:

- 1) x must be a decimal number between 224 and 239,
- 2) y, z, and w must be decimal numbers between 0 and 255

Meaning: At **Monitor > MVR > Groups Information** you entered an invalid entry in the "add group address" field.

Recovery:

1. At **Monitor > MVR > Groups Information** enter a valid entry in the "add group address" field.
2. See the "[Monitor > MVR > Groups Information](#)" section.

Problem: Lost management of S4224***S4224 receiving excess broadcast packets causes loss of management***

Meaning: High amount of broadcast packets received on a port will cause loss of management of the S4224. This happens, even when STP is blocking the port which is the source of broadcasts, and when QoS Storm Control feature is configured to limit broadcast packets as low as 1pps.

S4224 Configuration: STP is enabled (default settings) and QoS Storm Control is enabled (broadcast, multicast, and unicast all limited to low value such as 1pps).

After connecting the S4224 to the broadcast storm, it's usually still manageable for several seconds. During this time period before loss of management, observe the following:

1. STP usually changes the storming port state to blocking.
2. CPU utilization goes to 99-100% (even when the storming port is discarding).
3. Port Statistics show massive amounts of packets received on the storm port (even when the storming port is discarding).

Eventually management of the S4224 is completely lost, until it's physically disconnected from the storm. At times, the S4224 is unresponsive even after disconnecting it from the storm, and has to be power cycled to regain management. Disabling Storm Control produces the same results.

Note that when the S4224 is connected to the storming switch, the storm appears to remain confined to just one S4224 port; storm traffic does not spread to other S4224 ports.

Tests through the S4224 are successful and indicate line rate transfers, even while the S4224 is connected to the storm, and is un-manageable.

Recovery:

1. Contact TN Tech Support.

Message: There isn't any entry provide WEB service. Do you want to proceed anyway?

Meaning: At **Configuration > Security > Switch > Access Management** you enabled Access Management Configuration and clicked the Save button without first adding a new entry.

Recovery:

1. Click the **Cancel** button and add a new entry, or click the **OK** button and continue operation.
2. See "Access Management" on page [210](#).

Message: Please make sure the DHCP server connected on trust port?

Meaning: At **Configuration > Security > Network > DHCP > Relay** when you enabled Relay Mode and entered a Relay Server IP address, the system requires a DHCP server on a trusted port at the specified IP address.

Recovery:

1. Make sure the DHCP server is connected on a trust port.
2. See "DHCP Server" on page [324](#).

**Message: Board Type not found, probing enabled
Invalid configuration detected (Signature Check Failed)**

Meaning: The S4224 board type parameter could not be discovered.

Recovery:

1. Make sure the Device ID entry is valid.
2. If possible, reset the S4224 to factory defaults.
3. If possible, reboot the S4224.

Message: No port members for VLAN 1. Please check the delete button t delete VLAN from the list or add the members.

Meaning: You tried to delete a non-existent VLAN translation entry from a group.

Recovery:

1. Click the **OK** button to clear the message.
2. Re-enter the command with a different (existing) group.
2. Add port member to the group and re-try the operation.
3. Make sure you are not trying to delete VLAN 1. Deleting VLAN 1 causes issues with forwarding.
4. To make sure no ports belong to VLAN 1, and then add VLAN 1 with all ports set to the forbidden state.
5. See the **Delete VLAN Translation Group Entry** command for CLI information.

**Problem: CPU can be overloaded by broadcast packets, causing loss of management.
S4224 receiving excess broadcast packets causes loss of management.**

Meaning: S4224 CPU overload and loss of management occur even when STP is discarding all packets from the port that the broadcasts are from, and when QoS Storm Control is configured to limit broadcast packets to rates as low as 1pps.

Recovery:

1. Enable Loop Protection.
2. See "[Loop Protection Configuration](#)" on page 155.

Problem: Ingress Bandwidth profiling on Port doesn't allow for bursty TCP flows.

Meaning: The Port ingress policers work fine for traffic generation for normal L2 traffic streams. For TCP flow which is bursty in nature, the resultant bandwidth is very poor close to 10% of the set rate. The issue can be that the **token** bucket for port ingress policer may not be set correctly to accommodate for the bursts mainly for TCP control frames.

Recovery:

1. Use EPL service which allows for bursty traffic flow.
2. See "[Ethernet Services Configuration](#)" on page 286.

Problem: MEP not working over link aggregation.

Meaning: Protocols above the LAG layer don't seem to consider the LAG group as a logical port (e.g., SOAM over an aggregated link). A MEP does not view the LAG group as a logical port; for example, if you:

1. Create an EVC with all LAG groups' ports in NNI.
2. Create a LAG group.
3. Create MEPs on the EVC (e.g., EVPL) service on UNI and NNI ports. Note that since a MEP has a residence port attached to it even though it's an EVC MEP, this creates issue when the residence port is down and CCMs are to be carried over the other ports. This creates faults on the MEP, possibly because of the MAC address being used in the CCMs.

Recovery: This is a deployment issue.

1. Use MEP on EVC instead; this is orthogonal to any aggregation. For a service running over an aggregation, just add all port to the NNI.

Problem: DNS not updated when new DHCP address is granted

Meaning: When a new address is granted a device via a DHCP operation, the "A" and "PTR" records in DNS must be corrected to point at the new address. The Client (3280) should drive that by sending "Option 81" in with the DHCP request response. This doesn't appear to be happening on the 3280 as a ping to the DNS name will fail. The 'A' record maps a host name to an IP address and the 'PTR' record creates a pointer to the host for reverse lookups.

Recovery: FQDN option 81 refers to the Fully Qualified Domain Name (FQDN) Dynamic Host Configuration Protocol (DHCP) option (81). See Microsoft TechNet article # bb727018 at <http://technet.microsoft.com/en-us/library/bb727018.aspx>.

Message:

Connection received from 192.168.1.110 on port 7700 [04/01 12:36:07.613]

Read request for file <S4224-master.dat>. Mode OCTET [04/01 12:36:07.613]

Using local port 3505 [04/01 12:36:07.613]

<S4224-master.dat>: sent 6956 blks, 3561330 bytes in 4 s. 0 blk resent [04/01 12:36:11.081]

Meaning: Standard messages received from TFTPd32 Log Viewer tab.

Recovery: None; information only. Tftpd32 is an open source IPv6 ready application with free DHCP, TFTP, DNS, SNTP and Syslog servers, and a TFTP client. The TFTP client and server are compatible with TFTP option support (e.g., tsize, blocksize, and timeout). Some extended features (e.g., directory facility, security tuning, interface filtering; progress bars and early acknowledgments) enhance the TFTP protocol usability and transfer rate for both client and server. The included DHCP server provides unlimited automatic or static IP address assignment. Tftpd32 is also provided as a Windows service. Tftpd64 is the same application compiled as a 64 bits application. See the TFTPd32 FAQ at http://tftpd32.jounin.net/tftpd32_faq.html#static_DHCP_english.

Message: Peer MEP ID x is already in use

Meaning: At the **Configuration > MEP > MEP** Configuration menu path you tried to add a new peer MEP with an existing Peer MEP ID.

Recovery:

1. Click the **OK** button to close the webpage message.
2. Enter a new Peer MEP ID and click the **Save** button.
3. See the related section of the manual.

Message: The user name contains illegal characters Please use a combination of letters, numbers and underscores.

Meaning: At **Configuration > Security > Switch > Users** you entered an unacceptable character in the User Name field.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Enter a new User Name without any spaces or other illegal characters and click the **Save** button.
4. See the “[Add a New User](#)” section on page 50.

Message: Entry with VLAN ID: x and MAC Address xx-xx-xx-xx-xx-xx already in MAC table.

Meaning: At the **Configuration > MAC Table > Static MAC Table Configuration** menu path, you tried to add a new static entry with a VLAN ID and MAC address that was already used.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. Enter a new static entry with a VLAN ID and MAC Address that is not already used.
3. Click the **Save** button.
4. See “[MAC Address Table Configuration](#)” on page 260.

Problem: Management Port EtherType 9100 does not function

Meaning: When Management Port EtherType Customer S-port is set to 9100, S4224 access via the MGMT port is lost. This is a known issue with a fix in process, available at the next S4224 version release.

Recovery:

1. Make sure you are running the latest version of S4224 software; upgrade if a newer version is available.
2. If possible, use the S4224 CONSOLE PORT.
3. If possible, use EtherType 88A8 or 8100. See the “[Ports](#)” description on page 225.
4. Verify the APS and MEP configurations.
5. Retry the operation.

Problem: When ERPS is configured using a separate APS and SF MEPs, the S4224 will crash. The separate APS MEP is configured with CCM disabled and APS enabled.

Meaning: This is a known issue with a fix in process; available at the next S4224 version release.

The S4224 boot script runs, and a series of messages displays:

```
Warning: conf_sec_open failed or size mismatch, creating defaultsW erps 00:00:01
29/erps_init#1315: Warning: conf_sec_open failed or size
mismatch, creating defaultsW link_oam 00:00:01 29/eth_link_oam_init#3012: Warning:
conf_sec_open failed or size mismatch, creating
defaultsPassword:
Login in progress...
Invalid username or password!
Username: adminPassword:
Login in progress...
Welcome to Transition Networks Command Line Interface (v1.0).
Type 'help' or '?' to get help.
```

Recovery:

1. Check the IP configuration. At the CLI prompt type **ip conf** and press **Enter**.
3. Make sure you are running the latest version of S4224 software; upgrade if a newer version is available.
4. Verify the APS and MEP configurations. See the related sections of this manual.
5. Retry the operation.

Message: fis load fails after firmware upgrade. The 'fis load -d managed' fails with one of the following errors after firmware upgrade:

```
decompression error: invalid block type
decompression error: invalid stored block lengths
```

Meaning: Flash Corruption and SPI Bus Access bug.

Recovery:

1. Boot managed.bk and run the firmware upgrade again.
2. When running the firmware upgrade again does not work, reprogramming the flash image has worked. Contact TN Support for direction.

Problem: Auto Negotiation between a 2.5G port and a 1G port does not work in S4224 v1.0.

Meaning: A check was added '&& (conf->speed == VTSS_SPEED_1G)', but 2.5G was missed. The S4224 software reads the SFP module and configures the link accordingly. On some systems it is not possible to read the SFP module via the I2C interface and this is the reason for the faulty behavior. This is a known issue with a fix in process; available at the next S4224 version release.

Recovery:

1. Make sure you are running the latest version of S4224 software; upgrade if a newer version is available.
2. Verify the port and auto-negotiation configurations. See the related sections of this manual.
3. Retry the operation.

Problem: Security level 11 appears to be equivalent to level 1

Meaning: When running at security level 11, only commands that work at levels 1 - 4 will display via the help, and do not seem to be otherwise available. This is a known issue with a fix in process, available at the next S4224 version release.

Recovery:

1. Do not use Security Level 11. Use Levels 10 and 12-14 instead.

Problem: Can no longer HTTPS browse to S4224 after new certificate is generated

Meaning: Initially enabling HTTPS and browsing to the S4224 with HTTPS works. However, if a new certificate is generated, any web browser that previously navigated the S4224 via https (using the old certificate) can no longer HTTPS browse the S4224. This may be because when a new certificate is generated, it re-uses the original certificate's serial number. This is a known issue with a fix in process, available at the next S4224 version release.

Recovery:

1. Make sure you are running the latest version of S4224 software; upgrade if a newer version is available.
2. If possible, use the existing certificate.

Problem: The **Clear** button does not clear data.

Meaning: Using the **Clear** button does not clear data at **Monitor > Link OAM > Event Status**. This is a known issue with a fix in process, available at the next S4224 version release.

Recovery:

1. Make sure you are running the latest version of S4224 software; upgrade if a newer version is available.
2. Try using the **Refresh** and/or **Auto-refresh** buttons.
3. Try using the **Clear** button at **Monitor > Link OAM > Statistics**.
4. Adjust the configuration at **Configuration > Link OAM > Port Settings** or at **Configuration > Link OAM > Event Settings**.

Problem: The **Clear** button at **Configuration > Link OAM > Event Settings** causes issues.

Meaning: Clicking the **Clear** button from this menu path will reset to all zeros in Error Window and Error Threshold, but refreshing will display default values again and clear the data at **Monitor > Link OAM > Statistics**. This is a known issue with a fix in process, available at the next S4224 version release.

Recovery:

1. Make sure you are running the latest version of S4224 software; upgrade if a newer version is available.
2. If possible, do not use the **Clear** button.

Problem: **Port admin status shows as 'disabled'**.

Meaning: The Port Admin status always displays as 'disabled', even when it is actually enabled. This is a known issue with a fix in process, available at the next S4224 version release.

Recovery:

1. Make sure you are running the latest version of S4224 software; upgrade if a newer version is available.
2. If possible, ignore the status displayed.

Message: **Invalid number of peer's for this configuration**

Meaning: At **Configuration > MEP > MEP Configuration > Instance Configuration >** you clicked the **Save** button before adding any Peer MEPS.

Recovery:

1. Click the **OK** button to clear the webpage message.
2. At **Configuration > MEP > MEP Configuration > Instance Configuration >** add one or more valid Peer MEPS and then click the **Save** button.
3. See "[MEP Instance Configuration](#)".

Message: Invalid Firmware Image - The uploaded firmware image is invalid. Please use a correct firmware image.

Meaning: At **Maintenance > Software > Upload** you clicked the **Upload** button without first browsing to and selecting a valid S4224 firmware filename.

Recovery:

1. Click the browser **Back** button to return to the Firmware Update page.
2. Browse to and select a valid file to use for this upgrade (e.g., *S4224-v1.0.1.dat*).
3. At the 'Choose File to Upload' dialog box, click the **Open** button.
4. Click the **Upload** button.
5. At the web page message, select **OK** or **Cancel**.
6. The upgrade will proceed, or the message "*Firmware Upload Error - Flash is already updated with this image*" will display.
7. Refer to the "[Software Upload Procedure](#)" on page 535.

Message: Firmware Upload Error - Flash is already updated with this image

Meaning: You tried to update the S4224 with the current (existing) firmware version.

Recovery:

1. Click the browser **Back** button to return to the Firmware Update page.
2. Browse to and select a valid file to use for this upgrade (e.g., *S4224-v1.0.1.dat*).
3. At the 'Choose File to Upload' dialog box, click the **Open** button.
4. Click the **Upload** button.
5. At the web page message, select **OK** or **Cancel**.
6. The upgrade will proceed, or the message "*Firmware Upload Error - Flash is already updated with this image*" will display.
7. Refer to the "[Software Upload Procedure](#)" on page 535.

Message: Warning! Device will automatically reboot. Proceed with update now?

Meaning: Information message indicating that you initiated a firmware update from the **Maintenance > Software > Upload** menu path. This procedure transfers the uploaded firmware image to the S4224 flash component. The S4224 will restart after the update. **Note:** do not reset or power off the S4224 during this process.

Recovery:

1. Verify that you want to perform this firmware update and resultant reboot and click **OK**. Otherwise click **Cancel**.
2. Refer to the "[Software Upload Procedure](#)" on page 535.

Problem: The message "*System restart in progress - The system is now restarting. - Polling...*" displays continuously without completing.

Meaning: At **Maintenance > Restart Device > Are you sure you want to perform a Restart?** prompt, you selected **Yes** with the **Force Cool Restart** checkbox checked.

Recovery:

1. Press the keyboard **Esc** key.
2. Press the browser **Back** button.
3. Log out and then log back in to the S4224.
4. Log out of the S4224, close the browser session, and then log back in to the S4224.
5. Restart the S4224 from the **Maintenance > Restart Device** menu path.

Message: OUI should have 3 digit groups

Meaning: At the **Configuration > Voice VLAN > OUI** menu path, you entered an invalid Telephony OUI.

Recovery:

1. Click the **OK** button to clear the webpage message.

Message:

ERPS ID " + fld.value + " is already in use
Only one ERPS can be added for each Save operation
Port 0 and Port 1 can not be same
Port 0 APS MEP instance must not be zero
Port 0 APS MEP and Port 1 APS MEP can not be same
Port 0 instance must not be zero
Port 0 SF MEP instance must not be zero
Port 0 SF MEP and Port 1 SF MEP can not be same
Port 1 APS MEP instance must not be zero
Port 1 instance must not be zero
Port 1 SF MEP instance must not be zero
West port can be zero only for interconnected sub-ring

Meaning: You entered an invalid parameter at the **Configuration > ERPS** menu path.

Recovery:

1. Click the **OK** button to clear the webpage message (if applicable).
2. Re-enter the parameter within the valid range. See “[ERPS Instance Configuration](#)” on page 250. Note that the number refers to the MEP instance number and not the MEP ID (which may or may not be the same).
3. Click the **Save** button when done.

Message:

error in putting all port+vlan in forwarding mode
failing in putting blocked port in forwarding state
Error in enabling forwarding for group = erpg->group_id

Meaning: Protection switching can be triggered by fault conditions and external manual commands. The fault conditions include Signal Failure (SF) and Signal Degrade (SD), where:

sf_state : signal failure state on a given ring port

sd_state : signal degrade state of a given ring port (for future use)

An SD fault occurs when at least one of the links it forwarded through has rate of errored bits exceeding a predetermined BER threshold.

The default configuration is that all VLANs are disabled and all ports are discarding for all ERPS instances.

Recovery: If the application (ERPS module) enables a VLAN for an ERPS instance, it must set up the forwarding state for all ports for the instance.

Message: NAS Error

The 802.1X Admin State must be set to Authorized for ports that are enabled for Spanning Tree

Meaning: At **Configuration > Security > Network > NAS >** menu path you selected an unsupported NAS configuration for the existing Spanning Tree configuration.

Recovery:

1. Click the browser Back button to return to the **Configuration > Security > Network > NAS >** page.

2a. In the **Port Configuration** section in the **Admin State** column, select **Force Authorized**.

or:

2b. At **Configuration > Spanning Tree > CIST Ports** in the CIST Normal Port Configuration table in the STP Enabled column, uncheck the checkbox for the ports you want to set to other than **Force Authorized**.

3. Click the **Save** button.

4. At **Configuration > Security > Network > NAS >** menu path, in the **Port Configuration** section in the **Admin State** column, check the checkbox for the ports you want to set to other than Force Authorized (i.e., select Force Unauthorized, Port-based 802.1X, Single 802.1X, Multi 802.1X, or MAC-based Auth.).

Message: >E api 00:28:25 57/vtss_vcap_add#640: Error: VCAP ISI: Could not find ID: 2

E web 00:28:25 57/handler_config_evc_edit#311: Error: evc_mgmt_add(0): failed

Meaning: At the S4224 **Configuration > Ethernet Services** menu path, you tried to set up the ECE before setting up the related EVC.

At the CLI, you entered one of the EVC ECE commands before entering the related EVC commands.

Recovery: Set up the EVC before trying to set up the ECE.

Message: The new setting may lost some dynamic entries of port 2. Do you want to proceed anyway?

Meaning: At **Configuration > Security > Network > IP Source Guard > Static Table** you set a port configuration and clicked the **Save** button.

Recovery:

1. Click the **OK** button to continue or click **Cancel** to stop.

2. Make sure that this is the port configuration that you want. See **Configuration > Security > Network > IP Source Guard > Configuration** for more information.

Message: Switch does not respond.

There was a problem getting page data: Unknown

Meaning: One of the webpage messages above displays and the **Translate dynamic to static** button and the **Save** and **Reset** buttons are grayed out at the **Configuration > Security > Network > IP Source Guard > Configuration** page.

Recovery:

1. Click the **OK** button to clear the webpage message.

2. Re-enter the parameter within the valid range. See “[IP Source Guard Configuration](#)” on page 125.

3. Click the **Save** button when done.

4. Try the CLI command “**config default keep**” to restore the default setting but keep the assigned IP address, and then re-try the IP source guard operation.

Problem: When the FDB table reaches 8192 entries, a new dynamic MAC will be learned and override the old one.

Description: When the MAC table is full (8192 entries), the switch learns new entries and purges older entries even though these entries are not aged. This is the expected behavior. The MAC table is implemented so that it will always store the most active entries. The least recently used entries are removed to provide storage for new entries. The benefit of this approach is that in a normal network, flooding is kept to a minimum when the MAC table becomes full. This occurs even when aging is disabled. This behavior is not configurable.

Resolution:

1. Apply Port- or MAC-based authentication (IEEE802.1X).
2. Set up a per-port MAC table limit, preventing an intruder from taking up too much of the MAC table. For example, if a port is limited to 64 entries in the MAC table, frames causing this limit to be exceeded are discarded, and the MAC table is not affected.
3. Set up additional Storm Policers to prevent flooding on an unknown MAC address. See the **Configuration > QoS** section.

Problem: The "psec_limit" cannot work when configuration "limit" is "1024".

The S4224 fails to send the trap only when the limit control reaches '1024' at the 5 packets/sec. rate.

Also, some the highwarn and normal DMI traps occur when the limit parameter reaches '1023' or '1024'.

Description: This is a Port Security Limit Control issue where the software is unable to process the new Mac address frames in time. It is receiving frames faster than it can add to the Mac table and in turn looks like it is losing frames, thus not reaching the limit. In a normal scenario if new Mac addresses turns up for example, once a second, it will work. But in case of an attack of new Mac address, then the port won't shutdown, but it won't switch these frames either. The S4224 works fine when tested at 5 frames/second.

Resolution:

1. Decrease the limit to less than 200 (e.g., (**security network limit limit 194**)).
2. Check for upgrades with a fix to this known problem.

*Message: **Stack Communication Error** - A stack communication error occurred. Configuration changes may not have been applied. Please reload the switch selector list - the selected switch may have left the stack. Switch does not respond. Prevent this page from creating additional dialogs - OK*

Meaning: An internal error occurred during Flow Control configuration at the **Configuration > Port > Configuration** menu path. The 'current Rx/Tx' seems to be Link partner's ability for pause.

Recovery:

1. Check or uncheck the checkbox.
2. Click the **OK** button.

*Message: **The Connection has timed out***

Meaning: The S4224 switch can not communicate with the PC after enabling Flow Control from the **Configuration > Port > Configuration** menu path.

Recovery:

1. Change the MGMT port to 1522 as the default frame size. Increasing the CONSOLE PORT Max Frame size increased to tagged frame length fixes the problem.

Message: The value of 'Trap Destination Address' is 0.0.0.0. Do you want to proceed anyway?

Meaning: At the **Configuration > Security > Switch > SNMP > System** menu path you clicked the Save button without making an entry in the "Trap Destination Address" field.

Recovery:

1. If you want to enter a Trap Destination Address, click the **Cancel** button and make the entry.
If you want to proceed anyway, click the **OK** button.

Problem: 'System Restore Default' hangs intermittently and indefinitely.

Meaning: This appears to only happen when an EVC/ECE is configured. In S4224 v1.2.1 and above, EVC and ECE configurations are removed when you execute a System Restore via the web (**Maintenance > Configuration > Restore Binary**) or via the CLI (**config restore binary** command).

Recovery:

1. If the EVC/ECE is removed before defaulting then the command will not hang.
2. Upgrade the S4224 to the latest software version.

Problem: At **Configuration > Ethernet Services > Bandwidth Profiles** in the "Bandwidth Profiles Configuration" table, the numbers in the CIR (kbps) CBS (bytes) EIR (kbps) EBS (bytes) columns are different than expected.

Meaning: EVC BWP rates are now calculated from layer 2. Software versions 1.2.2 and before are based on Line rate (level 1) in BWP; versions 1.2.3 and above are based on Data rate (level 2) in BWP (per MEF CE2.0).

Recovery:

1. Reconfigure the "Bandwidth Profiles Configuration" table parameters.
2. See "[Configuration > Ethernet Services > Bandwidth Profiles](#)" on page 288.

Message:

Peer MAC is needed for HW based CCM.

peer MAC address should be unicast

Peer MAC should be unicast.

Meaning: The "Unicast Peer MAC" option only supports the unicast address to be configured.

Recovery:

1. Change the MEP configuration. See the "Peer MEP Configuration" section (**Configuration > MEP > MEP Configuration** menu path).
2. Retry the operation.

Message: *Setting Tx mirroring for mirror port (port %lu) has no effect. Tx mirroring ignored.*

Meaning: At **Configuration > Mirroring > Mirror Port Configuration** table, if you set an invalid value to the Mirroring Mode, this SNMP error displays.

Recovery:

1. Select a valid Mirror Mode entry (e.g., enable, disable, rx, or tx).
2. See "[Mirroring Configuration](#)" on page 316.

Message:

syslog Clear Level = %ld
syslog message get info fail!
syslog server address to set is: %s
Testing syslog number %d (prefix: Debug, Info, Warning, etc.)

Meaning: You entered an invalid Syslog entry.

Recovery:

1. Select a valid Syslog entry.
2. See “[Log \(System Log\) Configuration](#)” on page 32.

Message:

txt2ipv4 failed for tnIpAddr = %s (IP Mgmt Table Entry)
txt2ipv4 failed for tnSubnetMask = %s(IP Mgmt Table Entry)
Configuration failed (DefaultGateway table entry)
Meaning: An error occurred when configuring the DNS Server table.

Recovery:

1. Select a valid DNS entry at **Configuration > System > IP**.
2. See “[IP Configuration](#)” on page 18.

Message: >E api/cil 00:05:10 28/126_action_check#5539: Error: ACL policer and EVC policer can not both be enabled

Meaning: Two means of policers can not be enabled together.

Recovery:

1. Disable one or the other.

Message:

Error: Part of the VLAN configuration didn't apply as some of ports are in forbidden list for a given VLAN id.
Error: Part of the VLAN configuration didn't apply as some of ports are in member list for a given VLAN id.
notice: forbidden port cannot overlap with egress member port in MIB setting.

Meaning: The system does not allow changing VLAN member ports once there is forbidden port (or ports) in this VLAN.

Recovery:

1. Change either the VLAN member ports configuration or change the VLAN forbidden ports configuration.
2. See the “**Configuration > VLANs > VLAN Membership**” section of this manual.

Message:

Warning: FPGA 1.1 required
Warning: FPGA 2.x required

Meaning: The S4224 does not automatically reboot after FPGA upgrade, but should be rebooted to ensure proper operation.

Recovery: We recommend upgrading the FPGA first, then the software, because the unit will automatically reboot after the software upgrade. If upgraded in the reverse order (software then FPGA), you must manually reboot after the FPGA upgrade.

Message: Unable to Run

PTP clock is not created on Initiator.

Meaning: This is a PTP validation error. If PTP is not created and RFC2544 latency is chosen and you run the test, this error displays and the RFC2544 latency test will not run.

Recovery:

1. Configure a PTP clock instance to ensure accurate RFC 2544 Latency test step timestamps.
2. Make sure PTP is running on both devices to synchronize the Time of Day. See “[PTP Clock Configuration](#)” on page 316.
3. Retry the operation. See the RFC 2544 User Guide for more RFC2544 latency test information.

System Log Messages

The S4224 displays four levels of syslog messages as explained below. Note that the **All** level displays all three levels of information that the S4224 can logged (*Informational, Warning, Notice, and Error*).

Informational Level Messages

These are the Information level messages of the system log. These are normal operational messages used for reporting, measuring throughput, etc. This level of message requires no action.

Table 4: Syslog Informational Messages

| Info Level Message | Description |
|---|---|
| <i>SYS-BOOTING: Switch just made a cool boot.</i> | The S4224 was restarted. See "Maintenance > Restart Device" . |
| <i>Link up on port x</i> | The most recent link status on the port x is 'link up'. Port Link is up - no action needed. |
| <i>Link down on port x</i> | The most recent link status on the port x is 'link down'. See Configuration > Ports > Port Configuration . |
| <i>Using primary power source.</i> | Normal power on operation. |
| <i>Frame of 243 bytes received on port 1MAC</i> | Normal frame size information. |
| <i>Port 1 shut down</i> | Normal port shutdown information. |
| <i>Authentication for '%s' successful via '%s'</i> | Authentication was successful. |
| <i>User '%s' added</i> <i>User '%s' modified</i> <i>User '%s' removed</i> | The User config addition / change / delete was successful. |
| <i>Input Alarm 'd' triggered and message is 's'", alarm.description);</i> | An info level Alarm was triggered; see the "Alarms" section. |

Warning Level Messages

These messages are the Warning level of the system log. These Warning messages are not an error, but an indication that an error will occur if action is not taken (e.g. *file system 85% full*). Each item must be resolved within a given time.

Table 5: Syslog Warning Messages

| Warning Level Message | Description |
|---|--|
| <i>E api/cil 17:42:26</i> <i>29/26_action_check#6036:</i> | ACL policer and EVC policer can not both be enabled. Disable one or the other. |
| <i>Authentication for '%s' failed via '%s'</i> | Authentication failed. |
| <i>Input Alarm 'd' triggered and message is 's'", alarm.description);</i> | A warning level Alarm was triggered; see the "Alarms" section. |

Error Level Messages

Error level messages of the system log. These non-urgent failures should be relayed to a developer or an administrator. Each item must be resolved within a given time.

Table 6: Syslog Error Messages

| Error Level Message | Description |
|--|---|
| <i>E api/cil 17:42:45 29/126_acl_policer_free#6069:</i> | Error: policer 0 already free. The EVC policer or |
| <i>VLAN Port Configuration Ingress Filter Conflict - MSTP</i> | Verify the Ingress Policers, Port Policing, or Queue Policing configuration. See the Configuration > Security > Network > ACL or the Configuration > QoS menu path. |
| <i>VLAN Port Configuration Ingress Filter Conflict - ERPS</i> | Verify the VLAN Port and the ERPS configuration. See the related section of this manual. |
| <i>E web 03:15:49 58/handler_config_vlan#514: Error: vlan_mgmt_vlan_del(1): failed</i> | Verify the Management VLAN configuration. See the related section of this manual. |
| <i>E link_oam 00:27:32 58/eth_link_oam_mgmt_port_mib_retrival_oper_set#849: Error: Unable to retrieve the mode of the port(1/41)</i> | Verify the Link OAM Mib Retrieve settings. See the "Link OAM Mib Retrieve" section of this manual. Contact TN Support if necessary; see " Appendix D: Service, Warranty & Compliance Information " on page 614. |
| <i>Input Alarm 'd' triggered and message is 's', alarm.description);</i> | An error level Alarm was triggered; see the " Alarms " section. |

Note that the **All** level displays all three levels of information that the S4224 can log (*Info*, *Warning*, and *Error*).

Notice Level Messages

These messages are the Notice level of the system log. These Warning messages are not an error. Each item should be noted within a given time.

Table 7: Syslog Notice Messages

| Warning Level Message | Description |
|--|---|
| <i>LINK-UPDOWN: Interface Vlan 1, changed state to down.</i> | Link State changed to down for VLAN 1. |
| <i>LINK-UPDOWN: Interface GigabitEthernet 1/1, changed state to up.</i> | Link State changed to up for GbE interface. |
| <i>LINK-UPDOWN: Interface Vlan 1, changed state to up.</i> | Link State changed to down for VLAN 1. |
| <i>LINK-CHANGED: Interface GigabitEthernet 1/1, changed state to up (MEP).</i> | MEP state changed from down MEP to Up MEP. |

Third Party Program Messages

The S4224 displays error and information messages from various third party applications, such as Internet Explorer, HyperTerminal, PuTTY, etc. This section lists the messages, provides an example, and discusses the message meaning of and possible recovery steps.

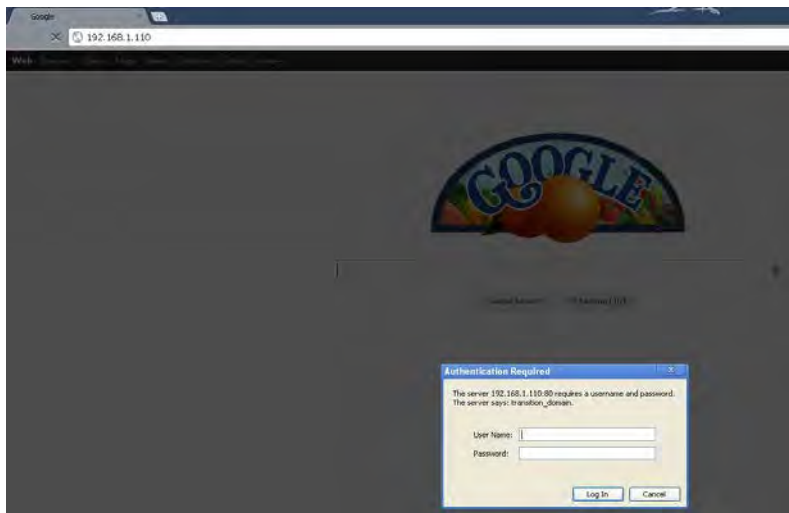
Message: PuTTY Security Alert - The server's host key is not cached in the registry.



Meaning: Normal PuTTY login security message.

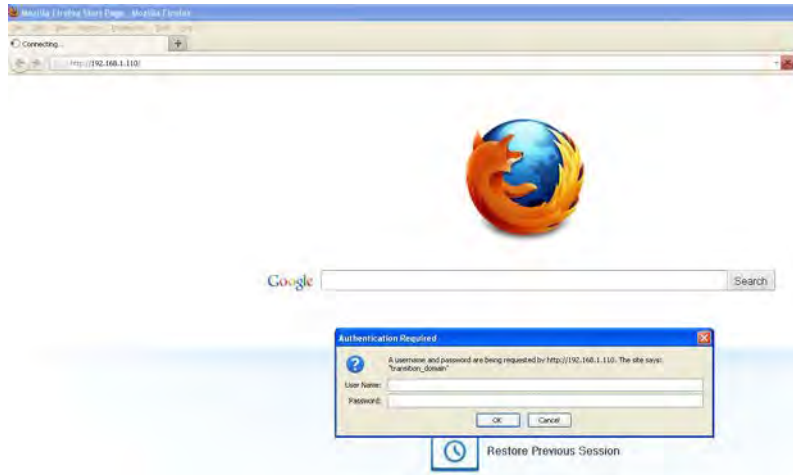
Recovery: Click the **Yes** button to trust this host, add the key to the PuTTY cache, and clear the message.

Message: Authentication Required



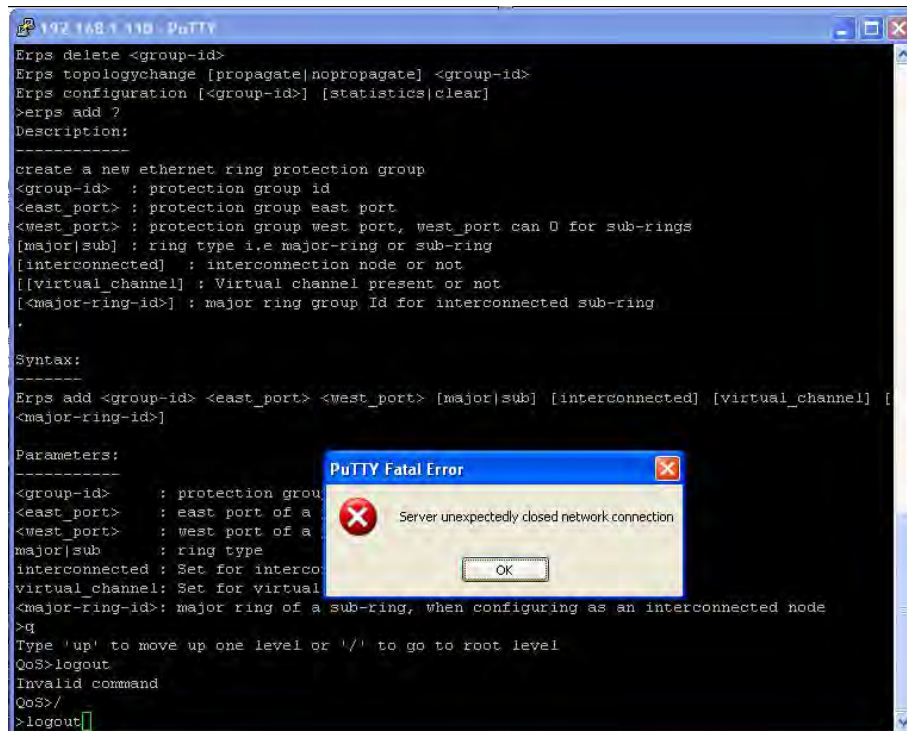
Meaning: Normal Google Chrome login screen.

Recovery: Enter your S4224 User Name and Password, and click the **Log In** button.

Message: Authentication Required

Meaning: Normal Firefox login screen.

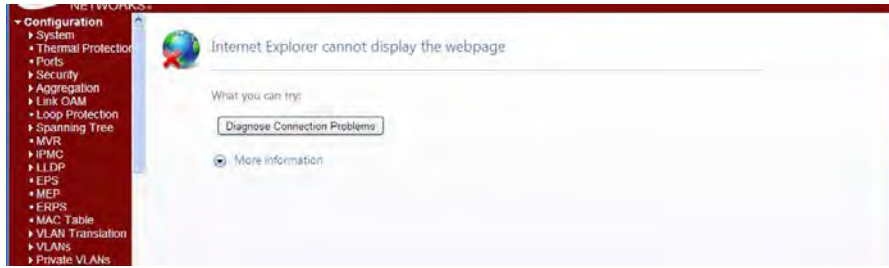
Recovery: Enter your S4224 User Name and Password, and click the **Log In** button.

Message: PuTTY Fatal Error - Server unexpectedly closed network connection

Meaning:

Recovery:

1. Click the **OK** button to close the message dialog box.
2. Close the PuTTY session window.
3. Start a new PuTTY session.

Message: Internet Explorer cannot display the webpage

Meaning: The S4224 web interface connection via Microsoft Internet Explorer is down.

Recovery:

1. Try reconnecting via the S4224 web interface in IE.
2. At the S4224 CLI prompt, press the **Enter** key.
3. Enter the CLI command “**config default keep_ip**” and press the **Enter** key. For example:

```
>config default keep_ip
>
```

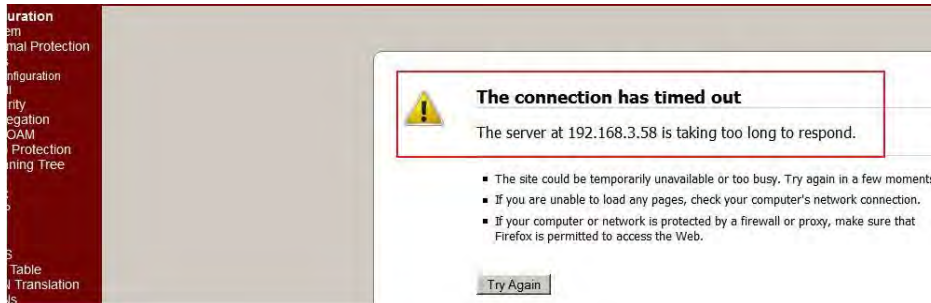
4. Try reconnecting in IE.
5. If necessary, try another supported web browser.

Problem: The S4224 screen locks up or displays incorrectly in Internet Explorer.

Description: Internet Explorer 9 has some glitches in its operations. Some web pages do not render correctly with IE because the web pages were designed for earlier functions.

Resolution:

1. Enable compatibility view in Internet Explorer (at IE > **Tools** > **Compatibility View**).
2. Continue operation.

Message: The Connection has timed out

Meaning: The S4224 switch can not communicate with the PC after enabling Flow Control from the **Configuration > Port > Configuration** menu path. Increasing the CONSOLE Port Max Frame size to the tagged frame length fixes the problem.

Recovery:

1. Change the MGMT port to 10056 as the default frame size.

Problem: A Reboot will stop Fault Management and Performance Management measurements.

Meaning: After a system reboot, the MEP PM and FM become disabled.

Recovery: At **Configuration > MEP > MEP Configuration**, re-enable the FM (LB, LT, TST, AIS, LCK) and PM (Loss Measurement and Delay Measurement) after a system Reboot.

Appendix A - Cables and Connectors

Cable Types

The cabling specifications are provided for troubleshooting purposes.

Copper (TP / UTP) CAT 1 – CAT 7 Cabling

ANSI/EIA Standard 568 is one of several standards that specify "categories" (each a "CAT") of twisted pair cabling systems. Assigned by the American National Standards Institute/Electronic Industries Association, these standards categories include CAT 1 – CAT 7, as shown below.

| Category | Max Data Rate | Typical Application |
|---------------------|---|---|
| CAT 1 | Up to 1 Mbps (1 MHz) | Analog voice (POTS), ISDN BRI |
| CAT 2 | 4 Mbps | IBM Token Ring network cabling systems |
| CAT 3 | 16 Mbps | Voice (analog mainly); 10BASE-T Ethernet |
| CAT 4 | 20 Mbps | Used in 16 Mbps Token Ring, but not much else. |
| CAT 5 | 100 MHz | 100 Mbps TPDDI. 155 Mbps ATM. No longer supported; replaced by 5E. 10/100BASE-T. |
| CAT 5E | 100 MHz | 100 Mbps TPDDI, 155 Mbps ATM, Gigabit Ethernet. Offers better near-end crosstalk than CAT 5. |
| CAT 6 | Up to 250 MHz | Minimum cabling required for data centers in TIA-942. CAT 6 is quickly replacing CAT 5e. |
| CAT 6E | Up to 500 MHz | Field-tested to 500 MHz. Supports 10 Gigabit Ethernet (10GBASE-T). May be either shielded (STP, ScTP, S/FTP) or unshielded (UTP). Standard published in Feb. 2008. The minimum requirement for Data Centers in the ISO Data Center standard. |
| CAT 7 (ISO Class F) | 600 MHz, 1.2 GHz in pairs with Siemon connector | Full-motion video, Teleradiology, Government and manufacturing environments. Fully Shielded (S/FTP) system using non-RJ45 connectors but backwards compatible with hybrid cords. Standard published in 2002. Until Feb. 2008, the only standard to support 10GBASE-T for a full 100m. |

CAT 7A/Class FA and Category 6A/Class EA specifications were published in February, 2008.

Fiber (10/100/1000BASE-xx) Cabling

The IEEE recommends the maximum fiber cable distances shown below.

| Standard | Data Rate (Mbps) | Cable Type | IEEE Standard Distance |
|-------------|------------------|---|------------------------|
| 10BASE-FL | 10 | 850nm Multimode 50/125 μ m or 62.5/125 μ m | 2 km |
| 100BASE-FX | 100 | 1300nm Multimode 50/125 μ m or 62.5/125 μ m | 2 km |
| 100BASE-SX | 100 | 850nm Multimode 50/125 μ m or 62.5/125 μ m | 300 m |
| 1000BASE-SX | 1000 | 850nm Multimode 50/125 μ m 850nm Multimode 62.5/125 μ m | 550 m 220 m |
| 1000BASE-LX | 1000 | 1300nm Multimode 50/125 μ m or 62.5/125 μ m 1310nm Single mode 9/125 μ m | 550 m 5 km |
| 1000BASE-LH | 1000 | 1550nm Single mode 9/125 μ m | 70 km |

Connector Types

The DMI connector type indicates the external optical or electrical cable connector provided as the interface. The information below is from SFF 8472 Rev 11.0. For additional information see the latest SFF-8472 Specification at <ftp://ftp.seagate.com/sff/SFF-8472.PDF>.

Table 8: Connector Descriptions

| Value | Description of connector |
|---------|--|
| 00h | Unknown or unspecified |
| 01h | SC |
| 02h | Fibre Channel Style 1 copper connector |
| 03h | Fibre Channel Style 2 copper connector |
| 04h | BNC/TNC |
| 05h | Fibre Channel coaxial headers |
| 06h | FiberJack |
| 07h | LC |
| 08h | MT-RJ |
| 09h | MU |
| 0Ah | SG |
| 0Bh | Optical pigtail |
| 0Ch | MPO Parallel Optic |
| 0D-1Fh | Unallocated |
| 20h | HSSDC II |
| 21h | Copper pigtail |
| 22h | RJ45 |
| 23h-7Fh | Unallocated |
| 80-FFh | Vendor specific |

The LC, MT-RJ, LC, SC, ST, or VF-45 connector types (jacks) are shown below.



ST



SC



LC



MT-RJ



VF-45

Figure 12. Connector Types

Appendix B - Licenses

This appendix provides S4224 license information. At the **Monitor > System > Information** menu path you can click the **Acknowledgments > Details** link to display the current set of source code from the various Open-Source components.

NOTICE

This system contains source code from the following Open-Source components. Some code has been altered to work with the embodying system.

[CPU-load](#): SVG graph
[Dropbear](#): SSH Server
[Host AP](#): EAPOL Authenticator and RADIUS authentication server
[ISC DHCP](#): DHCP Relay
[MD5](#): MD5 hash implementation
[MooTools](#): JavaScript Framework
[NET-SNMP](#): SNMP Agent
[NET-SNMP RMON](#): NET-SNMP RMON utilities
[NTP - Network Time Protocol](#): NTP Protocol
[OpenSSL](#): Toolkit implementing SSL v2/v3 and TLS protocols
[WPA Supplicant](#): EAP Peer state machines for MAC-based Authentication
[avltree](#): Self-balancing binary search tree
[eCos RTOS](#): Real-time OS for embedded applications
[libfetch](#): A library for retrieving and uploading files using Uniform Resource Locators (URLs).

| | |
|--------------|-----------|
| Name | CPU-load |
| Description | SVG graph |
| License type | BSD |

Copyright (C) 2004-2005 T. Lechat <dev@lechat.org>, Manuel Kasper <mk@neon1.net> and Jonathan Watt <jwatt@jwatt.org>.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

| | |
|--------------|-------------------|
| Name | Dropbear |
| Description | SSH Server |
| License type | MIT, BSD, OpenSSL |

Dropbear contains a number of components from different sources, hence there are a few licenses and authors involved. All licenses are fairly non-restrictive.

The majority of code is written by Matt Johnston, under the license below.

Portions of the client-mode work are (c) 2004 Mihnea Stoenescu, under the same license:

Copyright (c) 2002-2006 Matt Johnston
Portions copyright (c) 2004 Mihnea Stoenescu
All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

LibTomCrypt and LibTomMath are written by Tom St Denis, and are Public Domain.

=====

sshpty.c is taken from OpenSSH 3.5p1,
Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
All rights reserved

"As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell". "

=====

loginrec.c
loginrec.h
atomicio.h
atomicio.c
and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed under the 2 point BSD license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strlcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge,

publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

| | |
|--------------|--|
| Name | Host AP |
| Description | EAPOL Authenticator and RADIUS authentication server |
| License type | BSD |

Copyright (c) 2002-2012, Jouni Malinen <j@w1.fi> and contributors
All Rights Reserved.

This program is licensed under the BSD license (the one with advertisement clause removed).

License

This software may be distributed, used, and modified under the terms of BSD license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name(s) of the above-listed copyright holder(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

| | |
|--------------|------------|
| Name | ISC DHCP |
| Description | DHCP Relay |
| License type | ISC |

Copyright (c) 2004-2008 by Internet Systems Consortium, Inc. ("ISC")
Copyright (c) 1995-2003 by Internet Software Consortium

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES

WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Name MD5
Description MD5 hash implementation
License type BSD

Copyright (c) 2003-2005, Jouni Malinen <j@w1.fi>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License version 2 as published by the Free Software Foundation.

Alternatively, this software may be distributed under the terms of BSD license.

Name MooTools
Description JavaScript Framework
License type MIT

The MIT License

Copyright (c) 2006-2009 Valerio Proietti, <<http://mad4milk.net/>>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Name NET-SNMP
Description SNMP Agent
License type NET-SNMP (BSD-Style)

Various copyrights apply to this package, listed in 5 separate parts below. Please make sure that you read all the parts. Up until 2001, the project was based at UC Davis, and the first part covers all code written during this time. From 2001 onwards, the project has been based at SourceForge, and Networks Associates Technology, Inc hold the copyright on behalf of the wider Net-SNMP community, covering all derivative work done since then. An additional copyright section has been added as Part 3 below also under a BSD license for the work contributed by Cambridge Broadband Ltd. to the project since 2001. An additional copyright section has been added as Part 4 below also under a BSD license for the work contributed by Sun Microsystems, Inc. to the project since 2003.

Code has been contributed to this project by many people over the years it has been in development, and a full list of contributors can be found in the README file under the THANKS section.

---- Part 1: CMU/UCD copyright notice: (BSD like) ----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) ----

Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) ----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) ----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) ----

Copyright (c) 2003-2004, Sparta, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Name NET-SNMP RMON
 Description NET-SNMP RMON utilities
 License type Alex Rozin, Optical Access

Copyright (C) 2001 Alex Rozin, Optical Access

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation.

ALEX ROZIN DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL ALEX ROZIN BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Name NTP - Network Time Protocol
 Description NTP Protocol
 License type NTP

Copyright (c) David L. Mills 1992-2009

Permission to use, copy, modify, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright (c) 1990, 1993
 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Chris Torek.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
 1. Redistributions of source code must retain the above copyright

- notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
 3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the University of California, Berkeley and its contributors.
 4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1987, 1989 Regents of the University of California.
All rights reserved.

This code is derived from software contributed to Berkeley by
Arthur David Olson of the National Cancer Institute.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1983, 1993
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software

must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Amanda, The Advanced Maryland Automatic Network Disk Archiver
Copyright (c) 1991-1998 University of Maryland at College Park
All Rights Reserved.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of U.M. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. U.M. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

U.M. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL U.M. BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Author: James da Silva, Systems Design and Analysis Group
Computer Science Department
University of Maryland at College Park

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

| | |
|--------------|--|
| Name | OpenSSL |
| Description | Toolkit implementing SSL v2/v3 and TLS protocols |
| License type | OpenSSL |

Copyright (c) 2001 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

| | |
|--------------|--|
| Name | WPA Supplicant |
| Description | EAP Peer state machines for MAC-based Authentication |
| License type | BSD |

Copyright (c) 2003-2012, Jouni Malinen <jam@w1.fi> and contributors
All Rights Reserved.

This program is licensed under the BSD license (the one with advertisement clause removed).

License

This software may be distributed, used, and modified under the terms of BSD license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name(s) of the above-listed copyright holder(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

| | |
|--------------|-----------------------------------|
| Name | avltree |
| Description | Self-balancing binary search tree |
| License type | MIT |

Copyright (c) 2011 Bijal Thanawala

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

| | |
|--------------|--|
| Name | eCos RTOS |
| Description | Real-time OS for embedded applications |
| License type | Modified GPL |

This file is part of eCos, the Embedded Configurable Operating System. Copyright (C) 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009 Free Software Foundation, Inc.

eCos is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 or (at your option) any later version.

eCos is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with eCos; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

As a special exception, if other files instantiate templates or use macros or inline functions from this file, or you compile this file and link it with other works to produce a work based on this file,

this file does not by itself cause the resulting work to be covered by the GNU General Public License. However the source code for this file must still be made available in accordance with section (3) of the GNU General Public License v2.

This exception does not invalidate any other reasons why a work based on this file might be covered by the GNU General Public License.

Name libfetch
Description A library for retrieving and uploading files using Uniform Resource Locators (URLs).
License type Modified BSD

Copyright (c) 1998-2004 Dag-Erling Coïdan Smørgrav
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer in this position and unchanged.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Appendix C: Application Notes

S4224 Applications Support

The S4224 offers an unmatched level of Service Edge and Carrier Ethernet Networking features.

It provides a rich set of Carrier Ethernet switching features such as MEF Ethernet services, hierarchical QoS scheduling, provider bridging, protection switching, OAM, and Synchronous Ethernet.

The S4224 offers an unmatched level of Service Edge and Carrier Ethernet Networking features, and achieves wirespeed performance for even the most feature-rich Carrier Ethernet (CE) services.

The TN S4224 is an excellent choice for Mobile backhaul and for service provider demarcation points in Edge and Access devices

Key S4224 features include:

- MEF UNI and NNI functionality
- Hardware-based Ethernet OAM, performance monitoring, and service activation measurement (SAM)
- Network demarcation
- Hierarchical QoS priority for queuing and subscriber separation
- Service protection (linear, ring)
- Integrated timing with VeriTime™

S4224 applications include:

- Wireless and mobile backhaul (small cell)
- Ethernet demarcation

Available TN S4224 Application Notes

Application notes on certain specific functions / environments are available from your TN Technical Support specialist. Topics include:

1. Service OAM (SOAM)
2. Ethernet Services
3. QoS (Quality of Service)
4. L2 Protocols (LACP/LAG/MAC/VLAN/Mirroring/Remote Mirroring)

Not Intended for Use in Life Support Products: S4224 products are not intended for use in life support products, systems, or environments where failure of an S4224 product could reasonably be expected to result in death or personal injury. Anyone using an S4224 product in such an application without express written consent of an officer of Transition Networks, Inc. does so at their own risk, and agrees to fully indemnify Transition Networks, Inc. for any damages that may result from such use or sale.

Appendix D: Service, Warranty & Compliance Information

See the related Install Guide manual for:

- Service
- Warranty
- Compliance Information
- Declaration of Conformity
- Electrical Safety Warnings
- Safety Instructions for Rack Mount Installations
- other related S4224 information.













































































































Appendix E: SNMP Traps and MIBs

MIBs Supported

The following MIBs are supported per the CEServices spec:

- RFC1213 MIB II
- IEEE8021-Q BRIDGE MIB
- RFC 2819 RMON (Group 1,2,3, 9)
- RFC 2863 Interface Group MIB using SMIv2
- RFC 5519 Multicast Group Membership Discovery MIB
- RFC 3411 SNMP Management Frameworks
- RFC 3414 User-based Security Model for SNMPv3
- RFC 3415View-based access Control Model for SNMP
- RFC 3635 Ethernet-like MIB
- RFC 3636 802.3 MAU MIB
- RFC4133 Entity MIB v3
- RFC4188 Bridge MIB
- RFC4293 IP MIB
- RFC4668 RADIUS auth. Client MIB
- RFC4670 RADIUS Accounting MIB
- IEEE802.1 MSTP MIB
- IEEE802.3AB LLDP-MIB
- IEEE802.3ad LACP MIB
- IEEE802.1X PAE MIB
- TIA 1057 LLDP-MED
- RFC 4878 Link OAM MIB
- RFC 1215 TRAPS MIB
- RFC 2674 VLAN MIB

tn-mibs-v2.2.1.zip file

| \\tn-mibs-v2.2.x | \\standards | \\draft_standards |
|--|---|--|
| <ul style="list-style-type: none">  TN-ACL-MIB.smi  TN-ARP-INSPECTION-MIB.smi  TN-CES-MIB.smi  TN-CES-ROUTING-MIB.smi  TN-CONFIG-MIB.smi  TN-DEV-ACCESS-MGMT-MIB.smi  TN-DEV-AGGREGATION-MIB.smi  TN-DEV-SYS-IP2-MIB.smi  TN-DEV-SYS-IPMGMT-MIB.smi  TN-DEV-SYS-SNMPMGMT-MIB.smi  TN-DEV-SYS-UPGRADER-MIB.smi  TN-DEV-SYS-xNTP-MIB.smi  TN-DEV-VLAN-TRANSLATION-MIB.smi  TN-DHCP-MIB.smi  TN-ELPS-MIB.smi  TN-ENTITY-SENSOR-MIB.smi  TN-ERPS-MIB.smi  TN-ETHSOAM-MIB.smi  TN-ETHSOAM-PM-MIB.smi  TN-EVC-MIB.smi  TN-FRA-MIB.smi  TN-HTTPS-MIB.smi  TN-IPMC-SNOOPING-MIB.smi  TN-IP-SOURCE-GUARD-MIB.smi  TN-LINK-OAM-MIB.smi  TN-LLDP-EXT-MIB.smi  TN-LOAM-EXT-MIB.smi  TN-LOOP-PROTECT-MIB.smi  TN-MAC-MIB.smi  TN-MGMT-MIB.smi  TN-MGMT-TDM-MIB.smi  TN-MIRRORING-MIB.smi  TN-MRP-MIB.smi  TN-MVR-MIB.smi  TN-NAS-MIB.smi  TN-PORT-MIB.smi  TN-POWER-SUPPLY-MIB.smi <input type="checkbox"/> TN-Protection-MIB.mib  TN-PROV-MIB.smi  TN-PTP-MIB.smi  TN-PVLAN-MIB.smi  TN-QOS-EXT.smi  TN-RFC2544-MIB.smi  TN-SA-MIB.smi  TN-SAT-LOOPBACK-MIB.smi  TN-SECURITY-AAA-MIB.smi  TN-SECURITY-SWITCH-SSH-MIB.smi  TN-S-FLOW-MIB.smi  TN-SIP-MIB.smi  TN-SYNCE-MIB.smi  TN-SYS-LOG-MIB.smi <input type="checkbox"/> TN-SYSUSER-MIB.mib  TN-SYSUSER-MIB.smi  TN-THERMAL-PROTECTION-MIB.smi  TN-VLAN-MGMT-MIB.smi  TN-XSTP-MIB.smi  TN-ZERO-TOUCH-PROVISION-MIB.smi  TRANSITION-SMI.smi  TRANSITION-TC.smi | <ul style="list-style-type: none">  BRIDGE-MIB.smi  DOT3-OAM-MIB.smi  ENTITY-MIB.smi  ENTITY-STATE-TC-MIB.smi  EtherLike-MIB.smi  IANA-ADDRESS-FAMILY-NUMBERS-MIB.  IEC-62439-2-MIB.smi  IEEE8021-BRIDGE-MIB.smi  IEEE8021-CFM-MIB.smi  IEEE8021-CFM-V2-MIB.smi  IEEE8021-MSTP-MIB.smi  IEEE8021-PAE-MIB.smi  IEEE8021-Q-BRIDGE-MIB.smi  IEEE8021-SPANNING-TREE-MIB.smi  IEEE8021-TC-MIB.smi  IEEE8023-LAG-MIB.smi  IF-MIB.smi  IGMP-STD-MIB.smi  INET-ADDRESS-MIB.smi  IP-FORWARD-MIB.txt  IP-MIB.smi  LLDP-EXT-MED-MIB.smi  LLDP-MIB.smi  MAU-MIB.smi  MEF-SOAM-FM-MIB.smi  MEF-SOAM-PM-MIB.smi  MEF-SOAM-TC-MIB.smi  MGMT-MIB.smi  P-BRIDGE-MIB.smi  POE-MIB.smi  POWER-ETHERNET-MIB.smi  Q-BRIDGE-MIB.smi  RFC1213-MIB.smi  RFC4668-MIB.smi  RFC4670-RADIUS-ACC-CLIENT-MIB.smi  RMON2-MIB.smi  RMON-MIB.smi  SFLOW-MIB.smi  SMON-MIB.smi  SNMP-COMMUNITY-MIB.smi  SNMP-FRAMEWORK-MIB.smi  SNMP-MPD-MIB.smi  SNMP-NOTIFICATION-MIB.smi  SNMP-TARGET-MIB.smi  SNMP-USER-BASED-SM-MIB.smi  SNMPv2-MIB.smi  SNMPv2-SMI.smi  SNMPv2-TC.smi  SNMP-VIEW-BASED-ACM-MIB.smi | <ul style="list-style-type: none">  MEF-UNI-MIB.smi  PTP-MIB.smi |

The S4224 supports public (standard) and private Management Information Bases (MIBs).
The S4224 public MIBs are listed below.

Table 9: Public MIBs

| MIB | Note |
|--------------------------|---|
| RFC 1213 MIB II | MIB for Network Management of TCP/IP-based internets: MIB-II . Defines the second version of the MIB-II for use with network management protocols in TCP/IP-based internets. |
| IP-MIB | Request for Comments: 4293 . PROPOSED STANDARD; Errata Exist. One primary purpose of this revision of the IP MIB is to create a single set of objects to describe and manage IP modules in an IP version independent manner. |
| RFC 4188 Bridge MIB | Definitions of Managed Objects for Bridges. This RFC defines a portion of the MIB for use with network management protocols in TCP/IP-based internets. In particular, it defines objects for managing MAC bridges based on the IEEE 802.1D-1998 standard between LAN segments. Provisions are made for the support of transparent bridging. Provisions are also made so that these objects apply to bridges connected by subnetworks other than LAN segments. |
| RFC 2674 VLAN MIB | Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions. RFC 2674 defines two MIB modules for managing the new capabilities of MAC bridges defined by the IEEE 802.1D-1998 MAC Bridges and the IEEE 802.1Q-1998 Virtual LAN (VLAN) standards for bridging between LAN segments. One MIB module defines objects for managing the 'Traffic Classes' and 'Enhanced Multicast Filtering' components of IEEE 802.1D-1998. The other MIB module defines objects for managing IEEE 802.1Q VLANs. |
| RFC 4878 Link OAM MIB | Definitions and Managed Objects for OAM Functions on Ethernet-Like Interfaces. RFC 4878 defines objects for controlling link OAM functions and for providing results and status of the OAM functions to management entities. |
| IEEE 802.1AB (LLDP MIB) | 802.1AB-2009 - IEEE Standard for LANs/MANs-- Station and Media Access Control Connectivity Discovery defines a protocol and a set of managed objects that can be used for discovering the physical topology from adjacent stations in IEEE 802 LANs. |
| IEEE 802.1 (MSTP MIB) | IEEE 802.1™ : BRIDGING & MANAGEMENT; for the full set of IEEE Standards for Local and metropolitan area networks see http://standards.ieee.org/about/get/802/802.1.html . |
| IEEE 802.1X (PAE MIB) | 802.1X - Port Based Network Access Control; defines the changes necessary to the operation of a MAC Bridge in order to provide Port based network access control capability. |
| IEEE 802.30ad (LACP MIB) | Amendment to Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications-Aggregation of Multiple Link Segments. |
| RFC 2819 RMON | (Group 1, 2, 3 & 9.) Remote Network Monitoring MIB; defines a portion of the MIB for use with network management protocols in TCP/IP-based internets. In particular, it defines objects for managing remote network monitoring devices. |
| RFC 2613 SMON MIB | Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0; defines a portion of the MIB for use with network management protocols in TCP/IP-based internets. In particular, it defines objects for managing remote network monitoring devices in switched networks environments. |

| MIB | Note |
|-------------------------------------|--|
| RFC 2863 Interface Group MIB | The Interfaces Group MIB defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes managed objects used for managing Network Interfaces. |
| RFC 3635 Ethernet-like MIB | Definitions of Managed Objects for the Ethernet-like Interface Types; defines objects for managing Ethernet-like interfaces; it updates RFC 2665 by including management information useful for the management of 10 Gigabit per second (Gb/s) Ethernet interfaces. |
| RFC 3636 802.3 MAU MIB | Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs); defines objects for managing IEEE 802.3 MAUs; extends earlier specifications by including management information for the management of 10 gigabit per second (Gb/s) MAUs. |
| RFC 4133 Entity MIB version 3 | Entity MIB (Version 3) ; defines a portion of the MIB for use with network management protocols in the Internet community. It describes managed objects used for managing multiple logical and physical entities managed by a single SNMP agent. RFC 4133 specifies version 3 of the Entity MIB, which obsoletes version 2 (RFC 2737). |
| RFC 4668 RADIUS Auth. Client MIB | RADIUS Authentication Client MIB for IPv6; defines a set of extensions that instrument RADIUS authentication client functions. These extensions represent a portion of the MIB for use with network management protocols in the Internet community. Using these extensions, IP-based management stations can manage RADIUS authentication clients. RFC 4668 obsoletes RFC 2618 by deprecating the MIB table containing IPv4-only address formats and defining a new table to add support for version-neutral IP address formats. |
| RFC 3411 SNMP Management Frameworks | An Architecture for Describing SNMP Management Frameworks ; describes an architecture for describing Simple Network Management Protocol (SNMP) Management Frameworks. The architecture is designed to be modular to allow the evolution of the SNMP protocol standards over time. |
| SNMPv3 MPD | RFC 2572 (Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) describes the Message Processing and Dispatching for SNMP messages within the SNMP architecture [RFC2571]. It defines the procedures for dispatching potentially multiple versions of SNMP messages to the proper SNMP Message Processing Models, and for dispatching PDUs to SNMP applications. This document also describes one Message Processing Model - the SNMPv3 Message Processing Model. |
| RFC 3414 USM SNMPv3 | User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3); defines the Elements of Procedure for providing SNMP message level security. RFC 3414 also includes a MIB for remotely monitoring/managing the configuration parameters for this Security Model. |
| RFC 3415 VACM SNMPv3 | VACM (View-based Access Control Model) for the Simple Network Management Protocol (SNMP); defines the Elements of Procedure for controlling access to management information. This document also includes a MIB for remotely managing the configuration parameters for the View-based Access Control Model. RFC 3415 obsoletes RFC 2575. |
| IEEE 802.1AG MIB | The CFM (Connectivity Fault Management) standard specifies protocols, procedures, and managed objects to support transport fault management. These allow discovery and verification of the path, through bridges and LANs, taken for frames addressed to and from specified network users, detection, and isolation of a connectivity fault to a specific bridge or LAN. This standard will provide capabilities for detecting, verifying and isolating connectivity failures in networks. |

| MIB | Note |
|---------------------|--|
| MEF 31 (SOAM FM) | Service OAM Fault Management Definition of Managed Objects; specifies the Fault Management (FM) MIB necessary to implement the Service Operations, Administration, and Maintenance (OAM) that satisfies the Service OAM requirements and framework specified by MEF 17, the Service OAM Fault Management requirements as specified by SOAM-FM, and the Service OAM management objects as specified by MEF 7.1 which are applicable to FM functions. Two non-MEF documents serve as the baseline documents for this work: ITU-T Y.1731 and IEEE 802.1ag. |
| MEF SOAM PM (draft) | MEF 36 - Service OAM SNMP MIB for Performance Monitoring; specifies the Performance Monitoring (PM) MIB necessary to manage Service Operations, Administration, and Maintenance (OAM) implementations that satisfy the Service OAM requirements and framework specified by MEF 17, the Service OAM Performance Monitoring requirements as specified by SOAM-PM, and the Service OAM management objects as specified by MEF 7.1 which are applicable to PM functions. Two non-MEF documents serve as the baseline documents for this work: ITU-T Y.1731 and IEEE 802.1ag. |

The S4224 private MIBs are listed below.

Table 10: Private MIBs

| NO | MIB file | Table |
|----|-------------------------|--------------------------------------|
| 1 | TN-MGMT-MIB.sm i | tnEthInterfaceTable |
| 2 | TN-MGMT-MIB.sm i | tnDevSysCfgTable |
| 3 | TN-MGMT-MIB.sm i | tnDevSysMacLearningTable |
| 4 | TN-MGMT-MIB.sm i | tnDMInfoTable |
| 5 | TN-MGMT-MIB.sm i | tnIfLim idynMACLearningTable |
| 6 | TN-MGMT-MIB.sm i | tnIfDRTestTable |
| 7 | TN-MGMT-MIB.sm i | tnIfDRResultTable |
| 8 | TN-PROV-MIB | tnProvTable |
| 9 | TN-EVC-MIB | tnEvcPortTable |
| 10 | TN-EVC-MIB | tnEvcBandwidthProfilesTable |
| 11 | TN-VLAN-MGMT-MIB | tnSysManagmentVLANTable |
| 12 | TN-VLAN-MGMT-MIB | tnSysVLANExtTable |
| 13 | TN-VLAN-MGMT-MIB | tnIfVLANTagMgmtTable |
| 14 | P-BRIDGE-MIB | dot1dPortPriorityTable |
| 15 | P-BRIDGE-MIB | dot1dUserPriorityRegenTable |
| 16 | P-BRIDGE-MIB | dot1dTrafficClassTable |
| 17 | P-BRIDGE-MIB | dot1dPortOutboundAccessPriorityTable |
| 18 | ENTITY-MIB | entPhysicalTable |
| 19 | TN-DEV-SYS-UPGRADER-MIB | tnFirmwareUpgradeTable |
| 20 | TN-EVC-MIB | tnEvcTable |
| 21 | TN-EVC-MIB | tnEvcEceTable |
| 22 | TN-ETHSOAM-MIB | tnEthSoamMPTTable |
| 23 | IEEE8021-CFM-MIB | dot1agCfmMepTable |
| 24 | MEF-SOAM-FM-MIB | mefSoamLckCfgTable |
| 25 | MEF-SOAM-FM-MIB | mefSoamTestCfgTable |
| 26 | MEF-SOAM-FM-MIB | mefSoamTestStatsTable |
| 27 | MEF-SOAM-FM-MIB | mefSoamAisCfgTable |
| 28 | MEF-SOAM-FM-MIB | mefSoamLmCfgTable |
| 29 | MEF-SOAM-FM-MIB | mefSoamLbCfgTable |
| 30 | MEF-SOAM-FM-MIB | mefSoamLbMulticastTable |

| NO | M B file | Table |
|----|----------------------|-----------------------------------|
| 31 | TN-ETHSOAM-MB | tnEthSoamLocaCfgTable |
| 32 | TN-ETHSOAM-MB | tnEthSoamStatusTable |
| 33 | TN-ETHSOAM-MB | tnEthSoamLossStateTable |
| 34 | TN-ETHSOAM-MB | tnEthSoamTSExtfTable |
| 35 | TN-ETHSOAM-MB | tnEthSoamPeerCfgTable |
| 36 | TN-ETHSOAM-MB | tnEthSoamPeerStatusTable |
| 37 | TN-ETHSOAM-MB | tnEthSoamClientCfgTable |
| 38 | TN-ETHSOAM-MB | tnEthSoamLtmTable |
| 39 | TN-ETHSOAM-MB | tnEthSoamLtrfTable |
| 40 | IEEE8021-CFM-MB | dot1agCfmLtrfTable |
| 41 | TN-ETHSOAM-MB | tnEthSoamAisCfgTable |
| 42 | TN-ETHSOAM-MB | tnEthSoamDmCfgTable |
| 43 | TN-ETHSOAM-MB | tnEthSoamDmStateTable |
| 44 | TN-QOS-EXT-MB | tnQosExtPortPolicerfTable |
| 45 | TN-QOS-EXT-MB | tnQosExtPortQueuePolicerfTable |
| 46 | TN-QOS-EXT-MB | tnQosExtPortSchedulerfTable |
| 47 | TN-QOS-EXT-MB | tnQosExtPortSchedulerWeightfTable |
| 48 | TN-QOS-EXT-MB | tnQosExtPortShaperfTable |
| 49 | TN-QOS-EXT-MB | tnQosExtPortQueueShaperfTable |
| 50 | TN-QOS-EXT-MB | tnQosExtPortStormControlfTable |
| 51 | TN-DEV-SYS-IPMGMT-MB | tnIpMgmtfTable |
| 52 | TN-DEV-SYS-IPMGMT-MB | tnDnsServerfTable |
| 53 | TN-DEV-SYS-IPMGMT-MB | tnIpextMgmtfTable |
| 54 | TN-SYS-LOG-MB | tnSyslogMgmtfTable |
| 55 | TN-SYS-LOG-MB | tnSyslogMessageTable |
| 56 | TN-SYS-LOG-MB | tnSyslogExtfTable |
| 57 | TN-MIRRORING-MB | tnMirroringGroupTable |
| 58 | TN-MIRRORING-MB | tnMirroringIfTable |
| 59 | TN-LOOP-PROTECT-MB | tnLoopProtectBaseTable |
| 60 | TN-LOOP-PROTECT-MB | tnLoopProtectPortfTable |

For Additional MIB Information

For the list of S4224 SNMP Traps see “[SNMP v3 Traps](#) on page 70.

For information on Link OAM MIB Retrieval see [Diagnostics > Link OAM](#) on page 523.

For more information on the SNMP Agent, Network Management Station (NMS), MIBS, MIB modules and MIB Variables, the Object ID (OID), the MIB Tree / branch /node, MIB Table Indices, values, notations and transaction types, etc., see the SNMP Primer at <http://www.transition.com/pshelp/snmp.html#indices>.

The following sections detail S4224 configuration, monitoring, diagnostics, and maintenance via the S4224 web interface (menu system). See the S4224 CLI Reference manual for S4224 configuration, monitoring, diagnostics, and maintenance via the CLI (Command Line Interface).

SNMP Traps List

The table below lists and describes the Trap MIB variables.

Table 11: Traps List

| No | Trap MIB Variable | Binding | OID | Cause |
|----|--|--|-------------------------------|--|
| 1 | SNMPv2-MIB:coldStart | NULL | 1.3.6.1.6.3.1.1.5.1 | When the device undergoes a reboot. |
| 2 | SNMPv2-MIB:warmStart | NULL | 1.3.6.1.6.3.1.1.5.2 | <Not implemented> |
| 3 | SNMPv2-MIB:linkDown | 1: ifIndex 2: ifAdminStatus 3: ifOperStatus | 1.3.6.1.6.3.1.1.5.3 | When a port's link goes down due to adminstate change or due to physical layer connection. |
| 4 | SNMPv2-MIB:linkUp | 1: ifIndex 2: ifAdminStatus 3: ifOperStatus | 1.3.6.1.6.3.1.1.5.4 | When a port's link goes up. |
| 5 | SNMPv2-MIB:authenticationFailure | NULL | 1.3.6.1.6.3.1.1.5.5 | When SNMP community string sent in a request doesn't match the configured community string. |
| 6 | LLDP-MIB:lldpRemTablesChange | 1: lldpStatsRemTablesInserts 2: lldpStatsRemTablesDeletes 3: lldpStatsRemTablesDrops 4: lldpStatsRemTablesAgeouts | 1.0.8802.1.1.2.0.0.1 | When the topology of connected remote devices changes. |
| 7 | BRIDGE-MIB:newRoot | NULL | 1.3.6.1.2.1.17.0.1 | When the agent becomes the new Root of Spanning tree. |
| 8 | BRIDGE-MIB:topologyChange | NULL | 1.3.6.1.2.1.17.0.2 | When the status of configured ports in a Bridge changes from Learning to Forwarding state, or from Forwarding to Blocking state. |
| 9 | LLDP-EXT-MED-MIB:lldpXMedTopologyChangeDetected | 1: lldpRemChassisIdSubtype 2: lldpRemChassisId 3: lldpXMedRemDeviceClass | 1.0.8802.1.1.2.1.5.4795.0.1 | When a new remote device is connected or disconnect from the local device. |
| 10 | ENTITY-MIB:entConfigChange | NULL | 1.3.6.1.2.1.47.2.0.1 | When the device entity changes. |
| 11 | TN-MGMT-MIB:tnDMIRxIntrusionEvt | 1: ifIndex 2: tnDMIRxPwrLvlPreset 3: tnDMIRxPowerLevel | 1.3.6.1.4.1.868.2.5.3.0.1 | When the tnDMIRxPowerLevel falls below the tnDMIRxPwrLvlPreset, indicating an intrusion on the fiber. |
| 12 | TN-MGMT-MIB:tnDMIRxPowerEvt | 1: ifIndex 2: tnDMIRxPowerAlarm 3: tnDMIRxPowerLevel | 1.3.6.1.4.1.868.2.5.3.0.2 | When there is a warning or alarm on Rx Power. |
| 13 | TN-MGMT-MIB:tnDMITxPowerEvt | 1: ifIndex 2: tnDMITxPowerAlarm 3: tnDMITxPowerLevel | 1.3.6.1.4.1.868.2.5.3.0.3 | When there is a warning or alarm on Tx Power. |
| 14 | TN-MGMT-MIB:tnDMITxBiasEvt | 1: ifIndex 2: tnDMITxBiasAlarm 3: tnDMITxBiasCurrent | 1.3.6.1.4.1.868.2.5.3.0.4 | When there is a warning or alarm on Tx Bias current. |
| 15 | TN-MGMT-MIB:tnDMITemperatureEvt | 1: ifIndex 2: tnDMITempAlarm 3: tnDMITemperature | 1.3.6.1.4.1.868.2.5.3.0.5 | When there is a warning or alarm on DMI temperature. |
| 16 | TN-MGMT-MIB:tnFlLimitDynMACEvt | 1: ifIndex 2: tnFlLimitDynMACMaxCount 3: tnFlLimitDynMACState | 1.3.6.1.4.1.868.2.5.3.0.8 | When a port which has Limit control on dynamic MAC is enabled and the limit is reached. |
| 17 | TN-LOOP-PROTECT-MIB:tnLoopProtectLoopDetectedNotification | 1: ifIndex 2: tnLoopProtectPortLoopCount 3: tnLoopProtectPortAction | 1.3.6.1.4.1.868.2.5.22.0.1 | When a loop is detected in a port. |
| 18 | TN-ELPS-MIB:tnElpsAlarm | 1: tnElpsWFlowState 2: tnElpsPFlowState 3: tnElpsArchitectureMismatch 4: tnElpsAPSONWorking 5: tnElpsSwitchingIncomplete | 1.3.6.1.4.1.868.2.5.109.2.0.1 | When the configuration of EPS is modified. |
| 19 | NOTIFICATION-TYPE:tnThermalProtectionPortStatusChangedNotification | 1: ifIndex 2: tnThermalProtectionPriorityTemperature 3: tnThermalProtectionIfStatusTemperature 4: tnThermalProtectionIfStatusCode | 1.3.6.1.4.1.868.2.5.32.0.1 | A notification generated by the local device sensing a change in the thermal protection port status. The change indicates the current temperature of a port becomes higher (or lower) than its priority temperature. |

TN Private MIB OID Assignments

| OID | MIB module Name | OID | MIB module Name |
|----------------|------------------------|----------------|-------------------------|
| tnProducts.3 | tnMgmtMIB | tnProducts.120 | tnMRP |
| tnProducts.4 | tnVlanQoS MgmtMIB | tnProducts.121 | tnStaticIpRouting |
| tnProducts.6 | tnEntitySensorMIB | tnProducts.122 | tnSynceMIB |
| tnProducts.7 | tnLOAMExtMIB | tnProducts.123 | tnPtpMIB |
| tnProducts.9 | tnQosExtMIB | tnProducts.124 | tnUldMib |
| tnProducts.10 | tnDevSysIpMgmtMIB | tnProducts.125 | tnNASMIB |
| tnProducts.19 | tnSysCfgChangeMIB | tnProducts.126 | tnZeroTouchProvisionMIB |
| tnProducts.20 | tnPowerSupply | tnProducts.130 | tnEthSatLoopbackMIB |
| tnProducts.21 | tnFraMIB | tnProducts.137 | tnExtLldpMIB |
| tnProducts.22 | tnLoopProtectMIB | tnProducts.138 | tnAggCfgMIB |
| tnProducts.25 | tnMirroringMIB | tnProducts.140 | tnLinkOamMIB |
| tnProducts.26 | tnPrivateVlanMIB | tnProducts.141 | tnPortMIB |
| tnProducts.31 | tnIPSourceGuardMIB | tnProducts.142 | tnMacMib |
| tnProducts.32 | tnThermalProtectionMIB | tnProducts.143 | tnEthSoamPmMIB |
| tnProducts.33 | tnDhcpMIB | tnProducts.144 | tnMplsMib |
| tnProducts.35 | tnLacpMib | tnProducts.145 | tnHqosMib |
| tnProducts.50 | tnMVRMIB | tnProducts.146 | tnDhcpServerMib |
| tnProducts.60 | tnCesMIB | tnProducts.147 | tnDhcpSnoopingMib |
| tnProducts.61 | tnCesRoutingMIB | tnProducts.148 | tnDhcpRelayMib |
| tnProducts.105 | tnEthSoamMIB | tnProducts.149 | tnTtLoopMib |
| tnProducts.106 | tnEvcMIB | tnProducts.150 | tnRFC2544 |
| tnProducts.107 | tnEvcIdentityMIB | tnProducts.151 | tnLldpMib |
| tnProducts.108 | tnEtherSAT | tnProducts.154 | tnY1564 |
| tnProducts.109 | tnProtectionMIB | | |
| tnProducts.110 | tnProvMIB | | |
| tnProducts.111 | tnXstpMib | | |
| tnProducts.114 | tnIcmpSnoopingMib | | |
| tnProducts.115 | tnMldSnoopingMib | | |
| tnProducts.119 | tnSFlowMIB | | |

tnMgmtMIB subtree OID assignments

| OID | MIB module Name |
|---------------|---------------------|
| tnMgmtMIB.1.1 | tnDevMgmt |
| tnMgmtMIB.1.2 | tnInterfaceMgmt |
| tnMgmtMIB.1.3 | tnInterfaceDiagMgmt |
| tnMgmtMIB.1.4 | tnIfMACSecurityMgmt |
| tnMgmtMIB.1.5 | tnIfQOSMgmt |

tnDevMgmt subtree OID assignments

| OID | MIB module Name |
|--------------|------------------------|
| tnDevMgmt.1 | tnDevSysMgmt |
| tnDevMgmt.2 | tnDevSysLPT |
| tnDevMgmt.3 | tnDevSysDyingGasp |
| tnDevMgmt.4 | tnDevSysMACLearning |
| tnDevMgmt.5 | tnAcIMgmt |
| tnDevMgmt.11 | tnDevSysxNTP |
| tnDevMgmt.14 | tnDevSysSnmpmgmt |
| tnDevMgmt.18 | tnSyslogMIB |
| tnDevMgmt.19 | tnDevSysUser |
| tnDevMgmt.21 | tnSecurityAAAMIB |
| tnDevMgmt.22 | tnARPIInspectionMIB |
| tnDevMgmt.30 | tnDevSysUpgraderMIB |
| tnDevMgmt.36 | tnDevAccessMgmtMIB |
| tnDevMgmt.37 | tnDevVlanTranslation |
| tnDevMgmt.38 | tnDevAggregation |
| tnDevMgmt.42 | tnSecuritySwitchSSHMIB |
| tnDevMgmt.43 | tnHttpsMib |

TN Private MIBs

| # | MIB File | Table | Version |
|----|-------------------------|--------------------------------------|---------|
| 1 | TN-MGMT-MIB.smi | tnEthInterfaceTable | |
| 2 | TN-MGMT-MIB.smi | tnDevSysCfqTable | |
| 3 | TN-MGMT-MIB.smi | tnDevSysMacLearningTable | |
| 4 | TN-MGMT-MIB.smi | tnDMIIInfoTable | |
| 5 | TN-MGMT-MIB.smi | tnIfLimitDynMACLearningTable | |
| 6 | TN-MGMT-MIB.smi | tnIfDRTTestTable | |
| 7 | TN-MGMT-MIB.smi | tnIfDDRResultTable | |
| 8 | TN-PROV-MIB | tnProvTable | |
| 9 | TN-EVC-MIB | tnEvcPortTable | |
| 10 | TN-EVC-MIB | tnEvcBandwidthProfilesTable | |
| 11 | TN-VLAN-MGMT-MIB | tnSysManagementVLANTable | |
| 12 | TN-VLAN-MGMT-MIB | tnSysVLANExtTable | |
| 13 | TN-VLAN-MGMT-MIB | tnIfVLANTagMgmt2Table | |
| 14 | P-BRIDGE-MIB | dot1dPortPriorityTable | |
| 15 | P-BRIDGE-MIB | dot1dUserPriorityRegenTable | |
| 16 | P-BRIDGE-MIB | dot1dTrafficClassTable | |
| 17 | P-BRIDGE-MIB | dot1dPortOutboundAccessPriorityTable | |
| 18 | ENTITY-MIB | entPhysicalTable | |
| 19 | TN-DEV-SYS-UPGRADER-MIB | tnFirmwareUpgradeTable | |
| 20 | TN-EVC-MIB | tnEvcTable | |
| 21 | TN-EVC-MIB | tnEvcEceTable | |
| 22 | TN-ETHSOAM-MIB | tnEthSoamMPTable | |
| 23 | IEEE8021-CFM-MIB | dot1agCfmMepTable | |
| 24 | MEF-SOAM-FM-MIB | mefSoamLckCfqTable | |
| 25 | MEF-SOAM-FM-MIB | mefSoamTestCfqTable | |
| 26 | MEF-SOAM-FM-MIB | mefSoamTestStatsTable | |
| 27 | MEF-SOAM-FM-MIB | mefSoamAisCfqTable | |
| 28 | MEF-SOAM-FM-MIB | mefSoamLmCfqTable | |
| 29 | MEF-SOAM-FM-MIB | mefSoamLbCfqTable | |
| 30 | MEF-SOAM-FM-MIB | mefSoamLbrMulticastTable | |
| 31 | TN-ETHSOAM-MIB | tnEthSoamLocalCfqTable | |
| 32 | TN-ETHSOAM-MIB | tnEthSoamStatusTable | |
| 33 | TN-ETHSOAM-MIB | tnEthSoamLossStateTable | |
| 34 | TN-ETHSOAM-MIB | tnEthSoamTSExtTable | |
| 35 | TN-ETHSOAM-MIB | tnEthSoamPeerCfqTable | |
| 36 | TN-ETHSOAM-MIB | tnEthSoamPeerStatusTable | |
| 37 | TN-ETHSOAM-MIB | tnEthSoamClientCfqTable | |
| 38 | TN-ETHSOAM-MIB | tnEthSoamLtmTable | |
| 39 | TN-ETHSOAM-MIB | tnEthSoamLtrTable | |
| 40 | IEEE8021-CFM-MIB | dot1agCfmLtrTable | |
| 41 | TN-ETHSOAM-MIB | tnEthSoamAisCfqTable | |
| 42 | TN-ETHSOAM-MIB | tnEthSoamDmCfqTable | |
| 43 | TN-ETHSOAM-MIB | tnEthSoamDmStateTable | |
| 44 | TN-QOS-EXT-MIB | tnQosExtPortPolicerTable | |
| 45 | TN-QOS-EXT-MIB | tnQosExtPortQueuePolicerTable | |
| 46 | TN-QOS-EXT-MIB | tnQosExtPortSchedulerTable | |
| 47 | TN-QOS-EXT-MIB | tnQosExtPortSchedulerWeightTable | |
| 48 | TN-QOS-EXT-MIB | tnQosExtPortShaperTable | |
| 49 | TN-QOS-EXT-MIB | tnQosExtPortQueueShaperTable | |
| 50 | TN-QOS-EXT-MIB | tnQosExtPortStormControlTable | |
| 51 | TN-DEV-SYS-IPMGMT-MIB | tnIpMgmtTable | |
| 52 | TN-DEV-SYS-IPMGMT-MIB | tnDnsServerTable | |
| 53 | TN-DEV-SYS-IPMGMT-MIB | tnIpextMgmtTable | |
| 54 | TN-SYS-LOG-MIB | tnSyslogMgmtTable | |
| 55 | TN-SYS-LOG-MIB | tnSyslogMessageTable | |
| 56 | TN-SYS-LOG-MIB | tnSyslogExtTable | |
| 57 | TN-MIRRORING-MIB | tnMirroringGroupTable | |
| 58 | TN-MIRRORING-MIB | tnMirroringIfTable | |
| 59 | TN-LOOP-PROTECT-MIB | tnLoopProtectBaseTable | |
| 60 | TN-LOOP-PROTECT-MIB | tnLoopProtectPortTable | |
| 61 | TN-DEV-SYS-XNTP-MIB | tnxNTPServerTable | |

| | | | |
|-----|----------------------------|----------------------------------|------|
| 62 | TN-PRIVATE-VLAN-MIB | tnPVlanMembershipTable | |
| 63 | TN-PRIVATE-VLAN-MIB | tnPVlanPortIsolationTable | |
| 64 | TN-EVC-MIB | tnEvcL2cpCfgTable | v1.4 |
| 65 | IEEE8021-SPANNING-TREE-MIB | ieee8021SpanningTreeTable | v1.4 |
| 66 | IEEE8021-SPANNING-TREE-MIB | ieee8021SpanningTreePortTable | v1.4 |
| 67 | IEEE8021-MSTP-MIB | ieee8021MstpCistTable | v1.4 |
| 68 | IEEE8021-MSTP-MIB | ieee8021MstpCistPortTable | v1.4 |
| 69 | IEEE8021-MSTP-MIB | ieee8021MstpTable | v1.4 |
| 70 | IEEE8021-MSTP-MIB | ieee8021MstpPortTable | v1.4 |
| 71 | IEEE8021-MSTP-MIB | ieee8021MstpConfigIdTable | v1.4 |
| 72 | IEEE8021-MSTP-MIB | ieee8021MstpVlanTable | v1.4 |
| 73 | TN-XSTP-MIB | tnExtMstpCistTable | v1.4 |
| 74 | TN-XSTP-MIB | tnExtMstpTable | v1.4 |
| 75 | TN-XSTP-MIB | tnExtMstpCistPortTable | v1.4 |
| 76 | TN-XSTP-MIB | tnExtMstpPortTable | v1.4 |
| 77 | TN-XSTP-MIB | tnXstpPortStatsTable | v1.4 |
| 78 | TN-THERMAL-PROTECTION-MIB | tnThermalProtectionPriorityTable | v1.4 |
| 79 | TN-THERMAL-PROTECTION-MIB | tnThermalProtectionIfTable | v1.4 |
| 80 | TN-THERMAL-PROTECTION-MIB | tnThermalProtectionIfStatusTable | v1.4 |
| 81 | TN-ACCESS-MGMT-MIB | tnAccessMgmtCfgTable | v1.4 |
| 82 | TN-ACCESS-MGMT-MIB | tnAccessMgmtTable | v1.4 |
| 83 | TN-ACCESS-MGMT-MIB | tnAccessMgmtStatsTable | v1.4 |
| 84 | TN-IP-SOURCE-GUARD-MIB | tnIPSourceGuardTable | v1.4 |
| 85 | TN-IP-SOURCE-GUARD-MIB | tnIPSourceGuardIfTable | v1.4 |
| 86 | TN-IP-SOURCE-GUARD-MIB | tnIPSourceGuardStaticTable | v1.4 |
| 87 | TN-IP-SOURCE-GUARD-MIB | tnIPSourceGuardDynamicTable | v1.4 |
| 88 | TN-ARP-INSPECTION-MIB | tnARPInspectionConfigTable | v1.4 |
| 89 | TN-ARP-INSPECTION-MIB | tnARPInspectionPortModeTable | v1.4 |
| 90 | TN-ARP-INSPECTION-MIB | tnStaticARPInspectionTable | v1.4 |
| 91 | TN-ARP-INSPECTION-MIB | tnDynamicARPInspectionTable | v1.4 |
| 92 | SNMP-USER-BASED-SM-MIB | usmUser | v1.4 |
| 93 | SNMP-VIEW-BASED-ACM-MIB | vacmSecurityToGroupTable | v1.4 |
| 94 | SNMP-VIEW-BASED-ACM-MIB | vacmAccessTable | v1.4 |
| 95 | SNMP-VIEW-BASED-ACM-MIB | vacmMIBViews | v1.4 |
| 96 | TN-DEV-VLAN-TRANSITION-MIB | tnVlanTransPort1GroupMapTable | v1.4 |
| 97 | TN-DEV-VLAN-TRANSITION-MIB | tnVlanTransMapTable | v1.4 |
| 98 | SNMP-TARGET-MIB | snmpTargetAddrTable | v1.4 |
| 99 | SNMP-TARGET-MIB | snmpTargetParamsTable | v1.4 |
| 100 | SNMP-NOTIFICATION-MIB | snmpNotifyTable | v1.4 |
| 101 | SNMP-COMMUNITY-MIB | snmpCommunityTable | v1.4 |
| 102 | SNMP-COMMUNITY-MIB | snmpTargetAddrExtTable | v1.4 |
| 103 | DOT3-OAM-MIB | dot3OamEventLogTable | v1.4 |
| 104 | TN-SECURITY-AAA-MIB | tnAAAServerTable | v1.4 |
| 105 | TN-SECURITY-AAA-MIB | tnStatisticsTable | v1.4 |
| 106 | TN-DEV-SYS-IPMGMT-MIB.smi | tnIPv4MgmtTable | v1.4 |
| 107 | TN-DEV-SYS-IPMGMT-MIB.smi | tnIPv6MgmtTable | v1.4 |

Public MIBs

| MIB | Table | Version |
|----------------------------|---------------------------------------|----------------|
| RFC1213-MIB | system | 1.2.4 |
| RFC1213-MIB | sysORTable | 1.2.4 |
| RFC1213-MIB | interfaces | 1.2.4 |
| RFC1213-MIB | ifTable | 1.2.4 |
| RFC1213-MIB | ip | 1.2.4 |
| RFC1213-MIB | ipAddrTable | 1.2.4 |
| RFC1213-MIB | ipNetToMediaTable | 1.2.4 |
| RFC1213-MIB | ip | 1.2.4 |
| RFC1213-MIB | icmp | 1.2.4 |
| RFC1213-MIB | tcp | 1.2.4 |
| RFC1213-MIB | tcpConnTable | 1.2.4 |
| RFC1213-MIB | udp | 1.2.4 |
| RFC1213-MIB | udpTable | 1.2.4 |
| RMON2-MIB | etherStatsTable | 1.2.4 |
| RMON2-MIB | historyControlTable | 1.2.4 |
| RMON2-MIB | alarmTable | 1.2.4 |
| RMON2-MIB | 1.2.4 | 1.2.4 |
| IEEE8021-PAE-MIB | 1.2.4 | 1.2.4 |
| IEEE8021-PAE-MIB | 1.2.4 | 1.2.4 |
| IEEE8021-PAE-MIB | 1.2.4 | 1.2.4 |
| Q-BRIDGE-MIB | dot1qBase | 1.3.4 |
| Q-BRIDGE-MIB | dot1qFdbTable | 1.3.4 |
| Q-BRIDGE-MIB | dot1qTpFdbTable | 1.3.4 |
| Q-BRIDGE-MIB | dot1qTpGroupTable | 1.3.4 |
| Q-BRIDGE-MIB | dot1qStaticUnicastTable | 1.3.4 |
| Q-BRIDGE-MIB | dot1qStaticMulticastTable | 1.3.4 |
| Q-BRIDGE-MIB | dot1qVlanCurrentTable | 1.3.4 |
| Q-BRIDGE-MIB | dot1qVlanStaticTable | 1.3.4 |
| Q-BRIDGE-MIB | dot1qPortVlanTable | 1.3.4 |
| IEEE8021-Q-BRIDGE-MIB | ieee8021QBridgeTable | 1.3.4 |
| IEEE8021-Q-BRIDGE-MIB | ieee8021QBridgeFdbTable | 1.3.4 |
| IEEE8021-Q-BRIDGE-MIB | ieee8021QBridgeTpFdbTable | 1.3.4 |
| IEEE8021-Q-BRIDGE-MIB | ieee8021QBridgeTpGroupTable | 1.3.4 |
| IEEE8021-Q-BRIDGE-MIB | ieee8021QBridgeStaticUnicastTable | 1.3.4 |
| IEEE8021-Q-BRIDGE-MIB | ieee8021QBridgeStaticMulticastTable | 1.3.4 |
| IEEE8021-Q-BRIDGE-MIB | ieee8021QBridgeVlanCurrentTable | 1.3.4 |
| IEEE8021-Q-BRIDGE-MIB | ieee8021QBridgeVlanStaticTable | 1.3.4 |
| IEEE8021-Q-BRIDGE-MIB | ieee8021QBridgeNextFreeLocalVlanTable | 1.3.4 |
| IEEE8021-Q-BRIDGE-MIB | ieee8021QBridgePortVlanTable | 1.3.4 |
| IEEE8021-SPANNING-TREE-MIB | ieee8021SpanningTreeTable | 1.3.8 |
| IEEE8021-SPANNING-TREE-MIB | ieee8021SpanningTreePortTable | 1.3.8 |
| IEEE8021-MSTP-MIB | ieee8021MstpCistTable | 1.3.8 |
| IEEE8021-MSTP-MIB | ieee8021MstpCistPortTable | 1.3.8 |
| IEEE8021-MSTP-MIB | ieee8021MstpTable | 1.3.8 |
| IEEE8021-MSTP-MIB | ieee8021MstpPortTable | 1.3.8 |
| IEEE8021-MSTP-MIB | ieee8021MstpConfigIdTable | 1.3.8 |
| IEEE8021-MSTP-MIB | ieee8021MstpVlanTable | 1.3.8 |
| LLDP-MIB | lldpPortConfigTable | 1.3.8 |

| | | |
|-------------------------|--------------------------|--------|
| LLDP-MIB | lldpConfigManAddrTable | 1.3.8 |
| LLDP-MIB | lldpStatsTxPortTable | 1.3.8 |
| LLDP-MIB | lldpStatsRxPortTable | 1.3.8 |
| LLDP-MIB | lldpLocalSystemData | 1.3.8 |
| LLDP-MIB | lldpLocPortTable | 1.3.8 |
| LLDP-MIB | lldpLocManAddrTable | 1.3.8 |
| LLDP-MIB | lldpRemTable | 1.3.8 |
| LLDP-MIB | lldpRemManAddrTable | 1.3.8 |
| IEEE8023-LAG-MIB | dot3adAggTable | 1.3.8 |
| IEEE8023-LAG-MIB | dot3adAggPortListTable | 1.3.8 |
| IEEE8023-LAG-MIB | dot3adAggPortTable | 1.3.8 |
| IEEE8023-LAG-MIB | dot3adAggPortStatsTable | 1.3.8 |
| IEEE8023-LAG-MIB | lagMIBObjects | 1.3.8 |
| SNMP-USER-BASED-SM-MIB | usmUser | 1.3.10 |
| SNMP-VIEW-BASED-ACM-MIB | vacmSecurityToGroupTable | 1.3.10 |
| SNMP-VIEW-BASED-ACM-MIB | vacmAccessTable | 1.3.10 |
| SNMP-VIEW-BASED-ACM-MIB | vacmMIBViews | 1.3.10 |
| SNMP-TARGET-MIB | snmpTargetAddrTable | |
| SNMP-TARGET-MIB | snmpTargetParamsTable | |
| SNMP-NOTIFICATION-MIB | snmpNotifyTable | |
| SNMP-COMMUNITY-MIB | snmpCommunityTable | |
| SNMP-COMMUNITY-MIB | snmpTargetAddrExtTable | |

Additional SNMP traps notes:

- The Last Gasp can be in the form of IEEE802.3 2008 Clause 57 Dying gasp event and/or an SNMP trap to NMS system.
- The Y.1731 AIS and LCK faults for fault monitoring and isolation raise SNMP traps.
- All CCM errors such as remoteCCM, RDI, MACStatus, errorCCM, crossConnect, etc. are reported in MEP status and SNMP traps are raised for errors.
- SNMP traps are generated for various Threshold events (Errored Symbol Period, Errored Frame Event, Errored Frame Period Event and Errored Frame Seconds summary events) and Non-threshold events (dying gasp and critical events).
- The Link Fault, Dying Gasp, Critical Event, and other LOAM details for transmit and receive on each port are displayed at the **Monitor > Link OAM > Statistics** menu path.
- Dying Gasp is implemented as an SNMP trap and as a LOAM event.

SNMP Trap configuration is done at **Configuration > Security > Switch > SNMP > System**. See [SNMP System Configuration](#) on page 71.

Glossary

This section describes many of the terms and mnemonics used in this manual. Note that the use of or description of a term does not in any way imply support of that feature or of any related function(s).

1+1

The Protection Type 1+1 uses the protection resources at all times for sending a replica of the traffic. The protection merge point, where both copies are expected to arrive, decides which of the two copies to select for forwarding.

The decision can be to switch from one resource to the other due to an event like resource up/down etc. or can be on a per frame/cell basis, the selection decision is performed according to parameters defined below (e.g. revertive, non-revertive, manual, etc.).

A network can offer protection by providing alternative resources to be used when the working resource fails. The specific terminology for the number and arrangement of such resources includes 1+1, 1:1, 1:n, n:1, and m:n.

1:1

The 1:1 Protection Type provides a protection resource for a single working resource.

A network can offer protection by providing alternative resources to be used when the working resource fails. The terminology for the number and arrangement of such resources includes 1+1, 1:1, 1:n, n:1, and m:n.

1 PPS

In IEEE 1588v2, a pulse that is repeated every second and has a very accurate phase. It synchronizes several geographically dispersed clients (e.g., cell sites) to the same time and phase of 1 μ s. Any third party test equipment must also support 1 PPS.

A

AAA

(Authentication, Authorization and Accounting); examples of this type of protocols include RADIUS, TACACS, TACACS+, etc. See the IETF Working Group [status](http://tools.ietf.org/wg/aaa/) page (<http://tools.ietf.org/wg/aaa/>) for more information. For IETF RFC information see <http://tools.ietf.org/html/rfc2975>.

Authentication: refers to the process where an entity's identity is authenticated, typically by providing evidence that it holds a specific digital identity such as an identifier and the corresponding credentials. Examples of types of credentials are passwords, one-time tokens, digital certificates, and phone numbers (calling/called).

Authorization: determines whether a particular entity is authorized to perform a given activity, typically inherited from authentication when logging on to an application or service. Authorization may be determined based on a range of restrictions, for example time-of-day restrictions, or physical location restrictions, or restrictions against multiple access by the same entity or user. Typical authorization in everyday computer life is for example granting read access to a specific file for authenticated user. Examples of types of service include IP address filtering, address assignment, route assignment, quality of Service/differential services, bandwidth control/traffic management, compulsory tunneling to a specific endpoint, and encryption.

Accounting: refers to the tracking of network resource consumption by users for the purpose of capacity and trend analysis, cost allocation, billing.[3] In addition, it may record events such as authentication and authorization failures, and include auditing functionality, which permits verifying the correctness of procedures carried out based on accounting data. Real-time accounting refers to accounting information that is delivered concurrently with the consumption of the resources. Batch accounting refers to accounting information that is saved until it is delivered at a later time. Typical

information gathered includes the identity of the user or other entity, the nature of the service delivered, when the service began, when it ended, and if there is a status to report.

ACE

ACE (**A**ccess **C**ontrol **E**ntry) describes the access permission associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

ACL is an acronym for **A**ccess **C**ontrol **L**ist. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights. ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls. There are three S4224 web pages associated with the manual ACL configuration:

ACL | Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL | Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.

ACL | Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

ActiPHY™

An automatic power savings mode when a specific port is in link down or standby operation. ActiPHY® is a registered trademark used for Semiconductors, Integrated Circuits and Ethernet Transceivers and owned by Vitesse Semiconductor Corporation.

Address

Digital information that uniquely identifies a network, station, device, etc. so that each can send and receive messages. There are four types of addresses commonly used with the Internet:

- Email address (e.g., *name@mail_server.domain*)
- IP address or Internet address: *a.b.c.d* or *device_name.sub-domain.domain*
- MAC address (hardware address)
- URL (Uniform Resource Locator): *method://server_address[port]/document_path*

Address

In IPv6, an IPv6-layer identifier for an interface or a set of interfaces.

Alarm

The term 'alarm' actually refers to all types of fault events that are associated with a potential failure. Per MEF 15, the Perceived Alarm Severity (critical, major, minor, warning, indeterminate, or cleared). Severity assignments are only required for equipment alarms and physical layer communications alarms generated by the ME-NE).

- a. Critical - Indicates that a service affecting condition has occurred and immediate corrective action is required. Such a severity is used when the managed entity is totally out of service and its capability must be restored.
- b. Major - Indicates that a service affecting condition has occurred and urgent corrective action is required. Such a severity is used when there is a severe degradation in the capability of the managed entity and its full capability must be restored.

- c. Minor - Indicates that a non-service affecting condition has occurred and that corrective action should be taken in order to prevent a more serious fault.
- d. Warning - Indicates the detection of a potential or impending service affecting fault, before any significant effects have been felt.
- e. Indeterminate - The severity level cannot be determined.
- f. Cleared - The clearing of one or more previously reported alarms.

Anycast address

In IPv6, an identifier for a set of interfaces (typically belonging to different nodes). A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the "nearest" one, according to the routing protocol's measure of distance).

AES

AES is an acronym for **A**dvanced **E**ncryption **S**tandard. The encryption key protocol is applied in 802.11 standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

AP

Access Point, such as a wireless Access Point defined by IEEE 802.11.

APS

APS is an acronym for **A**utomatic **P**rotection **S**witching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

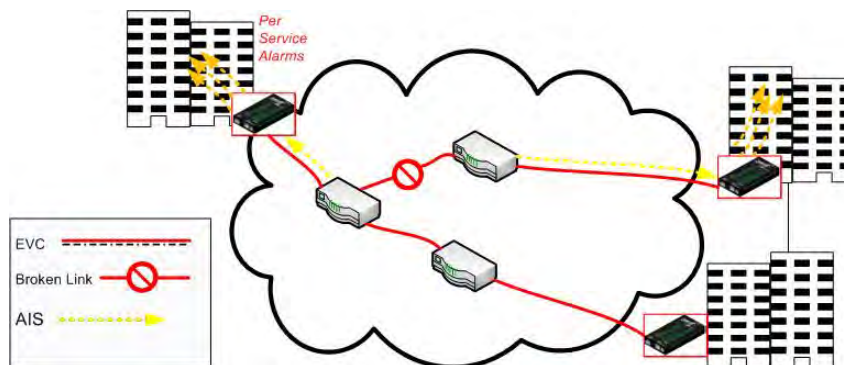
Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability. (Also *Port Aggregation*, *Link Aggregation*).

Alarm Indication Signal (AIS)

ETH-AIS allows alarm suppression when defects are to be detected at the server layer. You can enable or disable frames transmission with ETH-AIS information on a MEP or on a server MEP. You can also issue frames with ETH-AIS information at the client maintenance level by a MEP, including a server MEP, on detecting defect conditions. Defect conditions can include signal fail conditions with ETH-CC enabled, and AIS condition with ETH-CC disabled.

Only a MEP or Server MEP is configured to issue frames with ETH-AIS information. When a MEP detects a defect condition, it immediately starts transmitting periodic frames with ETH-AIS information at a configured client maintenance level. The MEP continues to transmit periodic frames with ETH-AIS information until the defect condition is resolved. On receiving a frame with ETH-AIS information, a MEP detects the AIS condition and suppresses loss of continuity alarms with all of its peer MEPs. The MEP resumes loss of continuity alarm generation on detecting loss of continuity conditions in place of the AIS condition.



Transmission of frames with ETH-AIS information can be enabled or disabled on a MEP (or on a server MEP). Frames with ETH-AIS information can be issued at the client MEG level by a MEP, including a server MEP, upon detecting defect conditions.

ARP

ARP is an acronym for **A**ddress **R**esolution **P**rotocol. It is a protocol that used to convert an **IP** address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Automatic Reversion

The protection is in revertive mode if, after a resource failure and its subsequent repair, the network automatically reverts to using this initial resource. The protection is in non-revertive mode otherwise. Automatic reversion may include a reversion timer (i.e., the Wait To Restore), which delays the time of reversion after the repair.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

B

Bandwidth Profile

A characterization of ingress Service Frame arrival times and lengths at a reference point and a specification of the disposition of each Service Frame based on its level of compliance with the Bandwidth Profile. In MEF documents, the reference point is the UNI. See [MEF 6.1](#).

Boundary clock

A clock that has multiple Precision Time Protocol (PTP) ports in a domain and maintains the timescale used in the domain. It may serve as the source of time (i.e., be a master clock) and may synchronize to another clock (i.e., be a slave clock).

A boundary clock is a clock with more than a single PTP port, with each PTP port providing access to a separate PTP communication path. Boundary clocks are used to eliminate fluctuations produced by routers and similar network elements.

BPDU

Bridge Protocol Data Units are data messages that are exchanged across the switches within an extended LAN that uses a spanning tree protocol topology. BPDU packets contain information on ports, addresses, priorities and costs and ensure that the data ends up where it was intended to go. BPDU messages are exchanged across bridges to detect loops in a network topology. The loops are then removed by shutting down selected bridge interfaces and placing redundant switch ports in a backup, or blocked, state.

Broadcast

A message forwarded to all (multiple, unspecified recipients) network destinations. On Ethernet, a broadcast packet is a special type of multicast packet where all nodes on the network are always willing to receive.

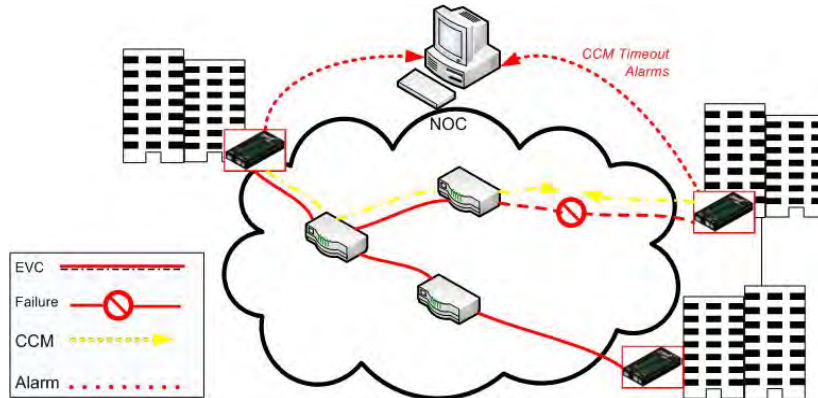
C

CC

CC (Continuity Check) is a [MEP](#) function that detects loss of continuity in a network by transmitting [CCM](#) frames to a peer MEP.

CC Monitoring (Continuity Checks Monitoring)

Fault detection uses the Continuity Check protocol to detect both connectivity failures and unintended connectivity between service instances. Each MEP can periodically transmit a multicast Connectivity Check Message (CCM) announcing the identity of the MEP and its MA, and tracks the CCMs received from the other MEPs. All connectivity faults that can misdirect a CCM show up as differences between the CCMs received and the MEP's configured expectations. The state of the tracked CCMs can be displayed.



Each Continuity Check Message (CCM) is a multicast CFM PDU transmitted periodically by a MEP to ensure continuity over the MA to which the transmitting MEP belongs. No reply is sent by any MP in response to receiving a CCM. CCMs use addresses from the Continuity Check Message Group Destination MAC Address table. The CCM can be sent away from or towards the MAC Relay Entity.

CCM

CCM is an acronym for **C**ontinuity **C**heck **M**essage. It is a **OAM** frame transmitted from a MEP to its peer MEP and used to implement **CC** functionality.

CDP

CDP (Cisco Discovery Protocol) is a Cisco proprietary Layer 2 protocol that is media- and protocol-independent, and runs on Cisco routers, bridges, access servers, and switches. A Cisco device with CDP enabled sends out periodic interface updates to a multicast address in order to make itself known to neighbors. As a layer two protocol, these packets (frames) are not routed. Using SNMP with the CDP MIB lets network management applications learn the device type and the SNMP agent address of neighboring devices, and to then send SNMP queries to those devices.

CIST

Acronym for **C**ommon and **I**nternal **S**pawning **T**ree. Concerning IST/CST/CIST, IST is the only instance that can send and receive BPDUs in the MST network. An MSTn instance is local to a region. ISTs in different regions are interconnected via a Common Spanning Tree (CST). The CIST includes the collection of ISTs in each MST region, and the CST that connects the ISTs.

The CIST is the default spanning tree instance of MSTP (i.e., all VLANs that are not members of particular MSTIs are members of the CIST). Also, an individual MST region can be regarded a single virtual bridge by other MST regions. The spanning tree that runs between MSTP regions is the CIST.

Clock

In PTP, a node participating in the Precision Time Protocol (PTP) that is capable of providing a measurement of the passage of time since a defined epoch.

Commonly Used EtherTypes

The 'EtherType' field in an Ethernet frame indicates the protocol used in the data field of the frame. According to the IEEE 802.3, Length/EtherType field is a two-octet field which takes one of two meanings, depending on its numeric value. For numeric evaluation, the first octet is the most significant octet; when the value of this field is ≥ 1536 decimal (0600 hex) the EtherType field indicates the nature of the MAC client protocol (EtherType interpretation). The value of the Type Field is obtained from the IEEE EtherType Field Registrar. The EtherType field is a very limited space and assignments are limited. The EtherType field is administered by the IEEE RAC EtherType Field Approval Authority.

The following list of EtherTypes is unverified information from various sources.

| EtherType (hex) | Protocol |
|------------------------|---|
| 0x000 - 0x05DC | IEEE 802.3 length |
| 0x0101-0x01FF | Experimental |
| 0x0600 | Xerox NS IDP |
| 0x0660, 0x0661 | DLOG |
| 0x0800 | IP (Internet Protocol) |
| 0x0801 | X.75 Internet |
| 0x0802 | NBS Internet |
| 0x0803 | ECMA Internet |
| 0x0804 | Chaosnet |
| 0x0805 | X.25 Level 3 |
| 0x0806 | ARP (Address Resolution Protocol) |
| 0x0808 | Frame Relay ARP (RFC 1701) |
| 0x6559 | Raw Frame Relay (RFC 1701) |
| 0x8035 | RARP (Reverse Address Resolution Protocol), DRAP (Dynamic RARP) |
| 0x80F3 | AARP, AppleTalk Address Resolution Protocol |
| 0x8100 | VLAN-tagged frame (IEEE 802.1Q) |
| 0x8137 | IPX (Internet Packet Exchange) |
| 0x814c | SNMP (Simple Network Management Protocol) |
| 0x86DD | IPv6 (Internet Protocol version 6) |
| 0x8808 | MAC Control |
| 0x8809 | Slow Protocols (IEEE 802.3) |
| 0x880B | PPP (Point to Point Protocol) |
| 0x880C | GSMP (General Switch Management Protocol) |
| 0x8819 | CobraNet |
| 0x8847 | MPLS (Multi-Protocol Label Switching) (unicast) |
| 0x8848 | MPLS (Multi-Protocol Label Switching) (multicast) |
| 0x8863 | PPoE (PPP over Ethernet) (Discovery stage) |
| 0x8864 | PPoE (PPP over Ethernet) (PPP Session stage) |
| 0x886F | Microsoft NLB heartbeat |
| 0x8870 | Jumbo Frames |
| 0x887B | HomePlug 1.0 MME |
| 0x888E | EAPOL (EAP over LAN) (IEEE 802.1X) |
| 0x88BB | LWAP (Light Weight Access Point Protocol) |
| 0x88CC | LLDP (Link Layer Discovery Protocol) |
| 0x8892 | PROFINET Protocol |
| 0x889A | HyperSCSI (SCSI over Ethernet) |
| 0x88A2 | ATA over Ethernet |
| 0x88A4 | EtherCAT Protocol |
| 0x88A8 | Provider Bridging (IEEE 802.1ad) |
| 0x88AB | Ethernet Powerlink |
| 0x88CC | LLDP |
| 0x88CD | SERCOS III |
| 0x88D8 | Circuit Emulation Services over Ethernet (MEF-8) |
| 0x88E1 | HomePlug AV MME |
| 0x88E5 | MAC security (IEEE 802.1AE) |
| 0x88F7 | Precision Time Protocol (IEEE 1588) |
| 0x8902 | IEEE 802.1ag Connectivity Fault Management (CFM) Protocol / ITU-T Recommendation Y.1731 (OAM) |
| 0x8906 | Fibre Channel over Ethernet |
| 0x8914 | FCoE Initialization Protocol |
| 0x9000 | Loopback (Configuration test protocol) |
| 0x9100 | VLAN Tag Protocol Identifier (Q-in-Q) |
| 0x9200 | VLAN Tag Protocol Identifier |
| 0xCAFE | Veritas LLT (Low Latency Transport) |

| | |
|--------|------------|
| 0xFFFF | (Reserved) |
|--------|------------|

Note: Some well known EtherTypes are not necessarily listed in the IEEE list of EtherType values. For example, EtherType 0x0806 (used by ARP) is listed by the IEEE only as "Symbolics, Inc., Protocol unavailable." See <http://standards.ieee.org/develop/regauth/ethertype/eth.txt> for more information.

The EtherType is one of two types of protocol identifier parameters that can occur in Ethernet frames after the initial MAC-48 destination and source identifiers. Ethertypes are 16-bit identifiers appearing as the initial two octets after the MAC destination and source (or after a tag).

EtherType use implies the use of the IEEE Assigned EtherType Field with IEEE Std 802.3, 1998 Edition Local and Metropolitan Area Networks. The EtherType Field provides a context for interpretation of the data field of the frame (protocol identification). Several well-known protocols already have an EtherType Field.

The IEEE 802.3, 1998 Length/EtherType Field, originally known as EtherType, is a two-octet field. When the value of this field is greater than or equal to 1536 decimal (0600 hexadecimal) the EtherType Field indicates the nature of the MAC client protocol (EtherType interpretation). The length and EtherType interpretations of this field are mutually exclusive.

Communication

In IPv6, any packet exchange among nodes that requires that the address of each node used in the exchange remain the same for the duration of the packet exchange. Examples are a TCP connection or a UDP request-response.

CoS

The QoS technique known as Class of Service (CoS) is a 3-bit field called the Priority Code Point (PCP) within an Ethernet frame header when using VLAN tagged frames as defined by IEEE 802.1Q. The PCP specifies a priority value of between 0 and 7 (inclusive) to be used by QoS disciplines to differentiate traffic. This technique is commonly referred to as IEEE 802.1p, but there is no IEEE standard or amendment under that name; the technique is incorporated into the IEEE 802.1Q standard, which specifies the tag inserted into an Ethernet frame.

Eight different classes of service can be expressed with the 3-bit PCP field in an IEEE 802.1Q header added to the frame. The way traffic is treated when assigned to any particular class is undefined by the spec and is left to the implementation. The IEEE however has made some broad recommendations:

| <u>PCP</u> | <u>Priority</u> | <u>Acronym</u> | <u>Traffic Types</u> |
|------------|-----------------|----------------|------------------------------------|
| 1 | 0 (lowest) | BK | Background |
| 0 | 1 | BE | Best Effort |
| 2 | 2 | EE | Excellent Effort |
| 3 | 3 | CA | Critical Applications |
| 4 | 4 | VI | Video, < 100 ms latency and jitter |
| 5 | 5 | VO | Voice, < 10 ms latency and jitter |
| 6 | 6 | IC | Internetwork Control |
| 7 | 7 (highest) | NC | Network Control |

Note that the above recommendation was revised in IEEE 802.1Q-2005, and it also differs from the original IEEE 802.1D-2004 recommendation. See also "QoS".

D

DA

(Destination Address); contrast SA.

DAD

(Duplicate Address Detection) - In IPv6, part of the NDP protocol that lets nodes check if an address is already in use.

DEI

DEI is an acronym for **D**rop **E**ligible **I**ndicator. It is a 1-bit field in the VLAN tag.

Deprecated address

In IPv6, an address assigned to an interface whose use is discouraged, but not forbidden. A deprecated address should no longer be used as a source address in new communications, but packets sent from or to deprecated addresses are delivered as expected. A deprecated address may continue to be used as a source address in communications where switching to a preferred address causes hardship to a specific upper-layer activity (e.g., an existing TCP connection).

DES

DES (**D**ata **E**ncryption **S**tandard) provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP (Dynamic Host Configuration Protocol) is a protocol used for assigning dynamic IP addresses to devices on a network. DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server. The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0). The parameter of "port_no" is the fourth byte and it means the port number. The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

DHCP Snooping is used to block intruders on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DMAC

(Destination MAC Address) A valid source MAC address, except for an address which has the lowest bit of the first byte set to '1'. These addresses, including the all 1's broadcast address FF:FF:FF:FF:FF:FF and the set of multicast addresses, are point-to-multipoint addresses and can never appear as the source address in an Ethernet frame. Note that a frame must be sent by a single source.

Each MAC header consists of three parts: 1. A 6-byte destination address, which specifies either a single recipient node (unicast mode), a group of recipient nodes (multicast mode), or the set of all recipient nodes (broadcast mode). 2. A 6-byte source address, which is set to the sender's globally unique node address. This may be used by the network layer protocol to identify the sender, but usually other mechanisms are used (e.g. ARP). Its main function is to allow address learning which may be used to configure the filter tables in a bridge. 3. A 2-byte type field, which provides a Service Access Point (SAP) to identify the type of protocol being carried. See also "SMAC".

DMI

Diagnostic Monitoring Interface; the S4224 is capable of supporting connectors with DMI (SFF-8472) capability. All DMI events will trigger notification. An intrusion detection based on Rx Power level is available for triggering any drop in the Rx power.

DNS

DNS (Domain Name System) stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

DoS is an acronym for **D**enial of **S**ervice. In a DoS attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets. An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

DSCP

DSCP (Differentiated Services Code Point) is a field in the header of IP packets for packet classification purposes. In an IP header, a six-bit DSCP field specifies the per-hop behavior for a given flow of packets. Each packet is given one of 64 possible forwarding behaviors (known as per-hop behaviors, or PHBs) for a given set of packet travel rules. DSCP uses the first 6 bits in the ToS field of the IPv4 packet header. In many cases, DSCP has replaced the outdated Type of Service (TOS) field.

Dual stack

One of three options for migrating to IPv6 from an existing IPv4 network infrastructure (dual-stack network, tunneling, and translation).

E

E911

Enhanced 911 Emergency Call Service applicable in North America.

EAPOL

The key protocol in 802.1x is called 'EAP over LANs' (EAPOL), which is currently defined for Ethernet-like LANs including 802.11 wireless, as well as token ring LANs (including FDDI).

In 802.1X, the user is called the 'supplicant', the switch is the 'authenticator', and the RADIUS server is the 'authentication server'. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. Note that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

The authenticator acts like a 'security guard' to a protected network. The supplicant (client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. The commonly used EtherType for EAPOL is 0x888E.

ECS

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

ECEs

(EVC Control Entries) The ECE ID identifies the ECE. Unique ECE IDs are automatically assigned to ECEs added. The possible range is from 1 through 128. See also "EVC".

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

ELIN

Emergency Location Identification Number, a valid North America Numbering Plan format telephone number, supplied to the PSAP for ECS purposes.

ENNI

(External Network-to-Network Interface) External Network to Network Interface; a reference point representing the boundary between two Operator MENs that are operated as separate administrative domains per MEF 26, 30. Previously "E-NNI".

Epoch

The origin of a PTP timescale.

EPS / ELPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU-T G.8031 (Ethernet (Linear) Protection Switch). Rec. ITU-T G.8031/Y.1342 (11/2009) defines the automatic protection switching APS protocol and linear protection switching mechanisms for point-to-point VLAN-based ETH SNC (Subnetwork Connection) in Ethernet transport networks. Protection switching occurs based on detection of certain defects on the transport entities (working and protection) within the protected domain. These defects are discussed in ITU-T G.8021.

The G.8031 Recommendation specifies linear protection switching mechanisms to be applied to VLAN-based Ethernet networks as described in G.8010. Protection switching is a fully allocated survivability mechanism ('fully allocated' in that the route and bandwidth of the protection entity is reserved for a selected working entity). EPS provides a fast and simple survivability mechanism. It is easier for a network operator to understand the network status (e.g., active network topology) with EPS than with other survivability mechanisms such as RSTP. G.8031 specifies linear 1+1 protection switching architecture and linear 1:1 protection switching architecture. The ETH-APS defined in Y.1731 is used as a signaling channel. [G.8031 \(2006\) Amd. 1 renamed EPS to ELPS](#).

ERP instance

An entity that is responsible for the protection of a subset of the VLANs that transport traffic over the physical Ethernet ring. Each ERP instance is independent of other ERP instances that may be configured on the physical Ethernet ring. Per ITU-T Rec.G.8032/Y.1344 (03/2010).

ERPS

ERPS is an abbreviation for Ethernet ring protection switching. Recommendation ITU-T G.8032/Y.1344 defines the automatic protection switching (APS) protocol and protection switching mechanisms for ETH layer Ethernet ring topologies. Included are details on Ethernet ring protection characteristics and architectures, and the Ring APS (R-APS) protocol. The protection protocol defined in this Recommendation enables protected point-to-point, point-to-multipoint and multipoint-to-multipoint connectivity within a ring or interconnected rings, called "multi-ring/ladder network" topology. The ETH layer ring maps to the physical layer ring structure.

The ERPS effort at ITU-T under G.8032 is to provide sub-50ms protection and recovery switching for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer. G.8032v1 supported a single ring topology and G.8032v2 supports multiple rings/ladder topology.

ERPS specifies protection switching mechanisms and a protocol for Ethernet layer network (ETH) rings. Ethernet Rings can provide wide-area multipoint connectivity more economically due to their reduced number of

links. The mechanisms and protocol defined in G.8032 provide highly reliable and stable protection; and avoid loops which would prove fatal to network operation and service availability.

Each Ethernet Ring Node is connected to adjacent Ethernet Ring Nodes participating in the same Ethernet Ring, using two independent links. A ring link is bounded by two adjacent Ethernet Ring Nodes, and a port for a ring link is called a ring port. The minimum number of Ethernet Ring Nodes in an Ethernet Ring is two. The basis of this RPS architecture are a) the principle of loop avoidance, and b) the use of learning, forwarding, and Filtering Database (FDB) mechanisms defined in the Ethernet flow forwarding function (ETH_FF).

Loop avoidance in an Ethernet Ring is done by guaranteeing that at all times, traffic may flow on all but one of the ring links. This particular link is called the Ring Protection Link (RPL), and under normal conditions this ring link is blocked (i.e., not used for service traffic). One designated Ethernet Ring Node, the RPL Owner Node, is responsible for blocking traffic at one end of the RPL. Under an Ethernet ring failure condition, the RPL Owner Node is responsible for unblocking its end of the RPL (unless the RPL has failed) allowing the RPL to be used for traffic. The other Ethernet Ring Node adjacent to the RPL, the RPL Neighbor Node, may also participate in blocking or unblocking its end of the RPL.

An Ethernet Ring failure results in protection switching of the traffic. This is achieved under the control of the ETH_FF functions on all Ethernet Ring Nodes. An APS protocol is used to coordinate the protection actions over the ring.

ERPS Performance

Note from Rec. ITU-T G.8032/Y.1344 (03/2010): "Ethernet ring protection switching performance: In an Ethernet ring, without congestion, with all Ethernet ring nodes in the idle state (i.e., no detected failure, no active automatic or external command, and receiving only "NR, RB" R-APS messages), with less than 1200 km of ring fibre circumference, and fewer than 16 Ethernet ring nodes, the switch completion time (transfer time as defined in [ITU-T G.808.1]) for a failure on a ring link will be less than 50 ms. On Ethernet rings under all other conditions, the switch completion time may exceed 50 ms (the specific interval is under study), to allow time to negotiate and accommodate coexisting APS requests. In case of interconnection of sub-rings with R-APS virtual channel to a major ring, the R-APS messages of the sub-ring that are inserted into the R-APS virtual channel take on performance characteristics (e.g., delay, jitter, packet drop probability, etc.) of the ring links and Ethernet ring nodes it crosses over the interconnected Ethernet ring. In this case, if the R-APS channel and R-APS virtual channel exceed the number of Ethernet ring nodes or fibre circumference defined above, the protection switching of the sub-ring may exceed 50 milliseconds. NOTE – The inclusion of the completion of FDB flush operation within the transfer time is for further study."

ESP

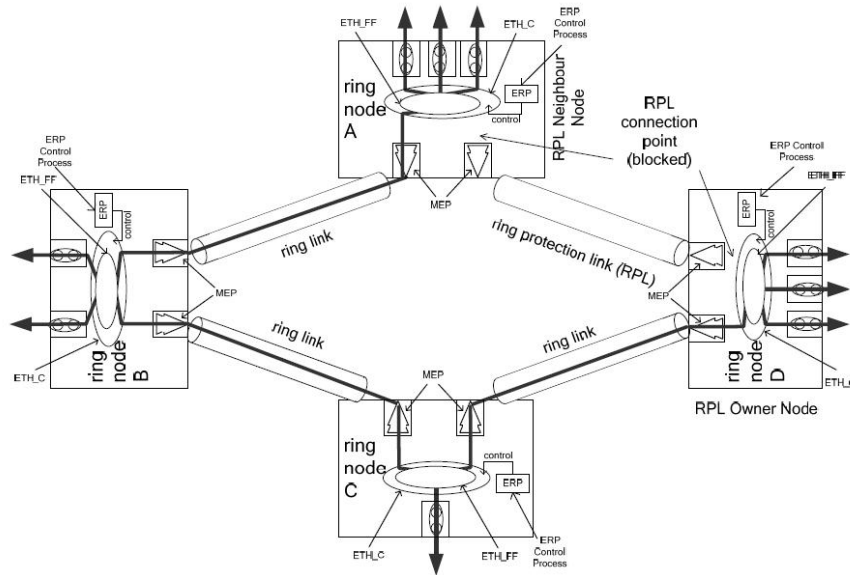
The IP Encapsulating Security Payload (ESP) protocol provides a mix of security services in IPv4 and IPv6. ESP supports two modes of operation: tunnel mode and transport mode.

The ESP header is designed to provide a mix of security services in IPv4 and IPv6. ESP may be applied alone, in combination with AH, or in a nested fashion.

Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host. The ESP header is inserted after the IP header and before the next layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode). ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality. The set of services provided depends on options selected at the time of Security Association (SA) establishment and on the location of the implementation in a network topology. See IETF [RFC 4303](#).

Ethernet ring

A collection of Ethernet ring nodes forming a closed physical loop whereby each Ethernet ring node is connected to two adjacent Ethernet ring nodes via a duplex communications facility. From ITU-T Rec.G.8032/Y.1344 (03/2010).



Ethernet ring node

A network element which implements at least the following functionalities:

- One Ethernet connection function (ETH_C) with a dedicated Ethernet flow forwarding function (ETH_FF) for forwarding ring automatic protection switching (R-APS) control traffic.
- Two ring ports, including ETHDi/ETH adaptation function at the ring maintenance entity group level (MEL).
- Ethernet ring protection (ERP) control process controlling the blocking and unblocking of traffic over the ring ports. Per ITU-T Rec.G.8032/Y.1344 (03/2010).

Ethernet Services

Generally refers to Metro Ethernet Services available from service providers (SPs) per MEF specifications (MEF 6, Ethernet Services Definitions, and MEF 10, Ethernet Services Attributes).

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame. See “Commonly Used EtherTypes” above.

EUI-64

The 64-bit Extended Unique Identifier (EUI-64) in IPv6.

EVC

(Ethernet Virtual Connection) An association of two or more UNIs that limits the exchange of frames to UNIs in the EVC. Generally, an EVC allows Ethernet service frames to be exchanged between UNIs that are connected via the same EVC. Per MEF 6.1, EVC performance requires “At least one CoS is REQUIRED. MUST specify CoS ID, per section 6.8 of [2]. MUST list values for each of the following attributes {Frame Delay, Frame Delay Variation, Frame Loss Ratio, and Availability} for each CoS, where Not Specified (N/S) is an acceptable value.”

F

Fast Leave

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

FCS

(Frame Check Sequence) per MEF 8, 11, 12.

flow

A given type of traffic sent between a producer device through a network to an endpoint known as a consumer. As the traffic goes through the network, it “flows” through the network. See also “Per flow QoS”.

Foreign master

An ordinary or boundary clock sending Announce messages to another clock that is not the current master recognized by the other clock.

FPGA

(Field-Programmable Gate Array) a chip that can be programmed in the field after manufacture.

FTP

FTP is an acronym for **F**ile **T**ransfer **P**rotocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

G

G-ACH

Generic Associated Channel (per IETF RFC5586)

GLAG

(Global Link Aggregation Group) is one of two supported types of Link Aggregation Groups. With GLAG, ports in a GLAG may reside on the same unit, up to two GLAGs are supported per stack, and each of the two GLAGs may consist of up to eight ports.

For both LLAGs and GLAGs, the egress port is chosen based on an ‘aggregation code’ that is calculated for the frame. This ensures that frames relating to a given frame flow are forwarded on the LLAG or GLAG member port, and thus do not risk being re-ordered. See also “LLAG”.

Global address

In IPv6, an address with unlimited scope.

Grandmaster clock

Within a PTP domain, a clock that is the ultimate source of time for clock synchronization using the protocol.

H

HMAC

(Hash-based Message Authentication Code) - a specific construction that calculates a message authentication code (MAC) involving a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. Any cryptographic hash function (e.g., MD5 or SHA-1) may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly. The cryptographic strength of the HMAC depends on the cryptographic strength of the underlying hash function, the size of its hash output length in bits, and on the size and quality of the cryptographic key.

Host

In IPv6, any node that is not a router.

HQoS

(Hierarchical Quality of Service) Queuing organized into 8 classes for each service on the port. HQoS provides more granular traffic control and quality assurance services than traditional QoS. HQoS uniformly manages traffic and "hierarchically" schedules traffic by user, network service, and application. HQoS manages traffic in scheduling 'queues' at multiple levels (physical, logical, application, or service level).

HQoS uses a forwarding 'class' as a scheduling entity (leaf node) in the scheduler policy 'tree'. A forwarding class corresponds to a scheduling queue, and packets are assigned to various scheduling queues according to specified mapping rules. The parameters tied to a forwarding class define the scheduling queue behavior. HQoS provides four forwarding classes; BE, AF, EF, and NC, where:

BE=Best Effort=Best-effort services, such as typical network browsing services.

AF=Assured Forwarding= Services guaranteeing transmission quality (e.g., VPN and data packet transmission).

EF=Expedited Forwarding=Delay/jitter-sensitive services (e.g., voice and video traffic transmission).

NC=Network Control=Highest-priority forwarding services (e.g., network control packet transmission).

HTTP

HTTP (Hypertext Transfer Protocol) is a protocol that used to transfer or convey information on the World Wide Web (WWW). HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) is used to indicate a secure HTTP connection. HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP (Internet Control Message Protocol) is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

ICMPv6

(Internet Control Message Protocol version 6) is the implementation of the Internet Control Message Protocol (ICMP) for Internet Protocol version 6 (IPv6) defined in RFC 4443.[1] ICMPv6 is an integral part of IPv6 and performs error reporting, diagnostic functions (e.g., ping), and a framework for extensions to implement future changes. Several extensions are published to define new ICMPv6 message types and options for existing ICMPv6 message types. The Neighbor Discovery Protocol (NDP) is a node discovery protocol in IPv6 that replaces and enhances functions of ARP. Secure Neighbor Discovery Protocol (SEND) is an extension of NDP with extra security. Multicast Router Discovery (MRD) allows discovery of multicast routers.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP (Internet Group Management Protocol) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP have three fundamental types of message as follows:

| Message | Description |
|--------------------|--|
| Query | A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group. |
| Report | A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message. |
| Leave Group | A message sent by a host to the querier to indicate that the host has quit to be a member of a specific multicast group. |

IGMP Querier

When a router sends IGMP Query messages onto a particular link, this router is called the 'Querier'. In order for IGMP, and thus IGMP snooping, to function, a multicast router must exist on the network and generate IGMP queries. The tables created for snooping (holding the member ports for a each multicast group) are associated with the querier. Without a querier the tables are not created and snooping will not work. Furthermore IGMP general queries must be unconditionally forwarded by all switches involved in IGMP snooping.[1] Some IGMP snooping implementations include full querier capability. Others are able to proxy and retransmit queries from the multicast router.

IGMP snooping

The process of listening to Internet Group Management Protocol (IGMP) network traffic. IGMP snooping, as implied by the name, is a feature that allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them. A switch will, by default, flood multicast traffic to all the ports in a broadcast domain (or the VLAN equivalent). Multicast can cause unnecessary load on host devices by requiring them to process packets they have not solicited. When purposefully exploited this is known as one variation of a denial-of-service attack. IGMP snooping is designed to prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. It provides switches with a mechanism to prune multicast traffic from links that do not contain a multicast listener (an IGMP client).

IGMP snooping allows a switch to only forward multicast traffic to the links that have solicited them. Essentially, IGMP snooping is a layer 2 optimization for the layer 3 IGMP. IGMP snooping takes place internally on switches and is not a protocol feature. Two standards organizations define IGMP snooping - the IEEE standardizes Ethernet switches, and the IETF standardizes IP multicast.

IMAP

IMAP (Internet Message Access Protocol) is a protocol for email clients to retrieve email messages from a mail server. IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

I-NNI

(Internal Network to Network Interface) per MEF 4. Internal NNI (this definition has not been implemented in any specification) per MEF 17.

Interconnection node

An Ethernet ring node which is common to two or more Ethernet rings or to a sub-ring and an interconnected network. At each interconnection node there may be one or more Ethernet rings that can be accessed through a single ring port and not more than one Ethernet ring that is accessed by two ring ports. The former set of Ethernet rings is comprised of sub-rings, whereas the latter Ethernet ring is considered a major ring, relative to this interconnection node. If the interconnection node is used to connect a (set of) sub-ring(s) to another network, then there is no Ethernet ring accessed by two ring ports. Per ITU-T Rec.G.8032/Y.1344 (03/2010).

Interface

In IPv6, a node's attachment to a link.

Interface identifier

In IPv6, a link-dependent identifier for an interface that is (at least) unique per link. Stateless address autoconfiguration combines an interface identifier with a prefix to form an address. In address autoconfiguration, an interface identifier is a bit string of known length. The exact length of an interface identifier and the way it is created is defined in a separate link-type specific document that covers issues related to the transmission of IP over a particular link type. In many cases, the identifier will be the same as the interface's link-layer address.

Invalid address

In IPv6, an address that is not assigned to any interface. A valid address becomes invalid when its valid lifetime expires. Invalid addresses should not appear as the destination or source address of a packet. In the former case, the internet routing system will be unable to deliver the packet, in the later case the recipient of the packet will be unable to respond to it.

IP

IP (Internet Protocol) is a protocol used for communicating data across an internet network. IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

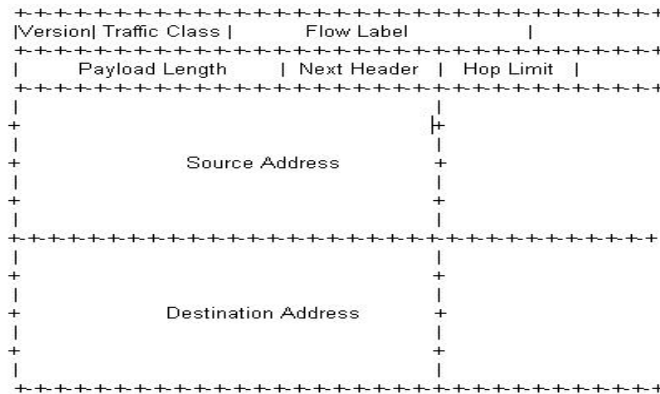
The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPv6

(Internet Protocol version 6) - The Version 6 IP protocol for Next Generation (IPng), a version of the Internet Protocol (IP) designed to succeed IPv4. The Internet operates by transferring data between hosts in small packets that are independently routed across networks as specified by an international communications protocol known as the Internet Protocol. Each host or computer on the Internet requires an IP address in order to communicate. The growth of the Internet has created a need for more addresses than are possible with IPv4. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with this long-anticipated IPv4 address exhaustion, and is described in Internet standard document RFC 2460, published in December 1998.[1] Like IPv4, IPv6 is an Internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks. While IPv4 allows 32 bits for an Internet Protocol address, and can therefore support 232 (4,294,967,296) addresses, IPv6 uses 128-bit addresses, so the new address space supports 2128 (approximately 340 undecillion or 3.4×10^{38}) addresses. This expansion allows for many more devices and users on the internet as well as extra flexibility in allocating addresses and efficiency for routing traffic. It also eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion. See IETF RFC2460.

IPv6 Header

The IPv6 Header format is shown below - from RFC 2460 - IPv6 Specification (Dec. 1998).



The IPv6 header fields are:

- **Version:** The 4-bit Internet Protocol version number (6).
- **Traffic Class:** An 8-bit traffic class field.
- **Flow Label:** A 20-bit flow label.
- **Payload Length:** the 16-bit unsigned integer. The Length of the IPv6 payload (i.e., the rest of the packet following this IPv6 header, in octets. Note that any extension headers present are considered part of the payload (i.e., included in the length count).
- **Next Header:** An 8-bit selector that identifies the type of header immediately following the IPv6 header. Uses the same values as the IPv4 Protocol field.
- **Hop Limit:** An 8-bit unsigned integer decremented by 1 by each node that forwards the packet. The packet is discarded if the Hop Limit is decremented to zero.
- **Source Address:** The 128-bit address of the originator of the packet.
- **Destination Address:** The 128-bit address of the intended recipient of the packet (possibly not the ultimate recipient, if a Routing header is present).

A full IPv6 implementation also includes these six extension headers: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, and Encapsulating Security Payload headers. Unlike IPv4, IPv6 nodes are not required to enforce a maximum packet lifetime, which is why the IPv4 "Time to Live" field was renamed "Hop Limit" in IPv6.

IPMC

IPMC (IP MultiCast) provides a means to talk to a group of hosts (a multicast group), where each host has a different MAC address, and at the same time ensure that other hosts, which are not part of the multicast group, don't process the information. Broadcast packets make use of a broadcast MAC address (FF:FF:FF:FF:FF:FF), which includes setting the broadcast/multicast bit in the address. (Unicast packets are delivered to a specific recipient on an Ethernet or IEEE 802.3 subnet by setting a specific layer 2 MAC address on the Ethernet packet address.) A multicast address is associated with a group of interested receivers. In IPv4, addresses 224.0.0.0 through 239.255.255.255 (the former Class D addresses) are designated as multicast addresses.[3] IPv6 uses the address block with the prefix ff00::/8 for multicast applications. In either case, the sender sends a single datagram from its unicast address to the multicast group address and the intermediary routers take care of making copies and sending them to all receivers that have joined the corresponding multicast group. IP multicast is a method of sending Internet Protocol (IP) datagrams to a group of interested receivers in a single transmission. It is often employed for streaming media applications on the Internet and private networks. The method is the IP-specific version of the general concept of multicast networking. It uses special reserved multicast address blocks in IPv4 and IPv6. In IPv6, IP multicast addressing replaces broadcast addressing as implemented in IPv4. The Linux commands *ping* and *netstat* are helpful when using IP multicast. Ping commands can be used for multicast addresses by providing a multicast address as argument. Running *netstat* with the *-g* option on a Linux system displays the set of all multicast groups that the Linux system has joined.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

J

Jumbo frames

The S4224 supports jumbo frames. This frame size is set to 10056 bytes or jumbo mode by default. The frame size is configurable to any value from 1500-9600 bytes. The jumbo mode is applicable only for data plane traffic; management and control plane traffic is still restricted to 1500 bytes.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The **L**ink **A**ggregation **C**ontrol **P**rotocol allows bundling several physical ports together to form a single logical port. LACP is used by neighboring devices to agree on adding links to a Link Aggregation Group, and to maintain packet ordering within each LAG. LACP will form an aggregation when 2 or more S4224 ports are connected to the same partner.

LCI

Location Configuration Information.

LER (Label Edge Routing)

A Label Edge Router makes a decision on which label to prefix to a packet and forwards. Also, the last router in the path removes the label from the packet and forwards the packet based on the header.

Link

In IPv6, a communication facility or medium over which nodes can communicate at the link layer (i.e., the layer immediately below IPv6). Examples are Ethernets (simple or bridged); PPP links; X.25, Frame Relay, or ATM networks; and internet (or higher) layer "tunnels", such as tunnels over IPv4 or IPv6 itself.

Link-layer address

In IPv6, a link-layer identifier for an interface. Examples include IEEE 802 addresses for Ethernet links and E.164 addresses for ISDN links.

Link-local Address

One of IPv6 addresses for local link usage. In IPv6, an address having link-only scope that can be used to reach neighboring nodes attached to the same link. All interfaces have a link-local unicast address.

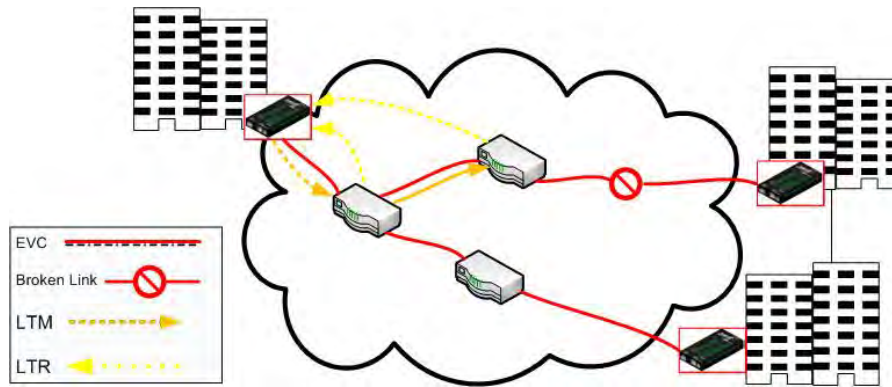
Link MTU

The IPv6 Maximum Transmission Unit - the maximum packet size in octets that can be conveyed over a link.

Link Trace

Link Trace messages are Multicast frames that a MEP transmits to track the path (hop-by-hop) to a destination MEP. Each receiving MEP sends a Linktrace Reply (LTR) directly to the Originating MEP, and regenerates the Linktrace Message: Each Linktrace Message (LTM) is a CFM PDU initiated by a MEP to trace a path to a target MAC address, forwarded from MIP to MIP, up to the point at which the LTM reaches its target, a MEP, or can no longer be forwarded. Each MP along the path to the target generates an LTR.

Each Linktrace Reply (LTR) is a unicast CFM PDU sent by an MP to a MEP, in response to receiving an LTM from that MEP. Linktrace Replies (LTRs) are carried in unicast frames. Linktrace Messages (LTMs) use addresses from the Linktrace Message Group Destination MAC Addresses table.



An LTM is used to signal to the MEP to transmit an LTM and to create an LTM entry in the MEP's Linktrace Database. The MA End Point can then be examined to determine whether or not the corresponding LTRs have been received by the MEP.

ETH-LT (Ethernet Link Trace) is an on-demand OAM function that can be used 1) to retrieve adjacency relationship between a MEP and a remote MEP or MIP, and 2) for Fault localization – when a fault (e.g., a link and/or a device failure) occurs, the sequence of MIPs and/or MEP will likely differ from the expected sequence. These differences provide information about the fault location.

ETH-LT request information is initiated in a MEP on an on-demand basis. After transmitting a frame with ETH-LT request information, the MEP expects to receive frames with ETH-LT reply information within a specified period of time. Network elements containing MIPs or MEPs and receiving the frame with ETH-LT request information respond selectively with frames containing ETH-LT reply information.

LLAG

(Local Link Aggregation Group) is one of two supported types of Link Aggregation Groups (same as Link Aggregation Group). With LLAG, all ports in an LLAG must reside on the same unit, any number of LLAGs may be configured for each unit in a stack, and each LLAG may consist of up to 16 ports. LLAGs are configured the same way as link aggregation groups for a standalone device (e.g., S4224).

For both LLAGs and GLAGs, the egress port is chosen based on an 'aggregation code' that is calculated for the frame. This ensures that frames relating to a given frame flow are forwarded on the LLAG or GLAG member port, and thus do not risk being re-ordered. See also "GLAG".

LLC

The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

LLDP

LLDP is an IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED Link Layer Discovery Protocol Media Endpoint Discovery. LLDP-MED is an extension of IEEE 802.1ab and is defined by the Telecommunication Industry Association (TIA-1057).

LLDPDU

Link Layer Discovery Protocol Data Unit, as defined in IEEE 802.1AB.

LOAM

(Link OAM) Ethernet Connectivity Fault Management (CFM) provided per IEEE 802.3ah OAM. The major features covered by this protocol are Discovery, Link Monitoring, Remote Fault Detection, and Remote Loopback. The S4224s support both Link layer OAM (LOAM, per IEEE 802.3-2005 Clause 57) and Service layer OAM (SOAM, per IEEE 802.1AG and Y.1731). Compare to “SOAM”.

LOC

LOC (Loss Of Connectivity) is detected by a MEP and indicates lost connectivity in the network. LOC can be used as a switch criteria by EPS.

M

MAC Swap

In SOAM testing, MEPs need to know about the device on the other side. They perform a MAC Swap so they can automatically populate the remote MAC Address to the test parameters. This is performed in Layer 2. See the S4224 **Configuration > MEP** menu path description.

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

Major ring

The Ethernet ring that is connected on two ports to an interconnection node. From ITU-T Rec.G.8032/Y.1344 (03/2010).

Master clock

In the context of a single PTP communication path, a clock that is the source of time to which all other clocks on that path synchronize. A system of 1588 clocks may be segmented into regions separated by boundary clocks. Within each region there will be a single clock, the master clock, serving as the primary source of time. These master clocks will in turn synchronize to other master clocks and ultimately to the grandmaster clock.

MD5

MD5 (Message-Digest algorithm 5) is a message digest algorithm used in a cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm. MD5 is an authentication protocol; one of two cryptography methods used for S4224 user authentication. MD5 is a widely used cryptographic hash function with a 128-bit hash value. Specified in RFC 1321, MD5 is used in a wide range of security applications, and is also commonly used to check file integrity. However, it has been shown that MD5 is not collision resistant; as such, MD5 is not suitable for applications like SSL certificates or digital signatures that rely on this property. MD5 was designed by Ron Rivest in 1991 to replace the earlier hash function MD4. See also “SHA”.

ME

(Maintenance Entity) An entity that requires management and is a relationship between two maintenance entity group (MEG) end points. MEs in Ethernet networks can nest but not overlap.

MED

Media Endpoint Discovery.

MEG

(Maintenance Entity Group) A ME Group (MEG) consists of the MEs that belong to the same service inside a common OAM domain.

MEG Level

The MEG Level is used to distinguish between OAM frames belonging to different nested MEs. MEs belonging to the same MEG share a common MEG Level. Eight MEG Levels have been identified for the purposes of Ethernet OAM.

When a Subscriber, Service Providers, and Network Operators share the MEG Levels space, allocation of MEG Levels can be negotiated between the various roles involved. A default allocation of MEG Levels is such that Service OAM frames for a Subscriber ME use MEG Level 7, 6 or 5; Service OAM frames for an EVC ME use MEG Level 3 or 4 as EVC ME belongs to a Service Provider OAM Domain; and Operator MEs use MEG Levels 2, 1, or 0. The MEG Levels used for UNI ME and NNI ME default to 0. Note that this default allocation of MEG Level space between Subscribers, Service Providers and Operators could change based on a mutual agreement between them.

MEG level of a MEP (0-7). The defaults per MEF 30 are:

| MEG | Default MEG Level | Suggested Use (MEF 30) |
|----------------------|--------------------------|--|
| Subscriber MEG | 6 | Subscriber monitoring of an Ethernet service. |
| Test MEG | 5 | SP isolation of subscriber reported problems. |
| EVC MEG | 4 | SP monitoring of provided service. |
| Service Provider MEG | 3 | SP Monitoring of Service Provider network. |
| Operator MEG | 2 | Netw. Operator monitoring of the portion of a network. |
| UNI MEG | 1 | Service Provider monitoring of a UNI. |
| ENNI MEG | 1 | Network Operators' monitoring of an ENNI. |

(where SP = Service Provider)

Note: Assignment of numerical MEG Levels to 'subscriber' (or customer) role, Service Provider role, and Operator role is somewhat arbitrary since those terms imply business relationships that cannot be standardized. For example, a 'subscriber' (or customer) may also be an Operator seeking a service from another Operator. The MEG Level default values are consistent with a shared MEG Level model across Subscriber, Operators, and Service Providers.

Note: The MEF and Broadband Forum (BBF) are not aligned on the use of MEG Level 5. If interworking between an MEF compliant implementation and a BBF compliant implementation is required, an agreement on the use of MEG Level 5 is required between the two parties.

MEP

A MEP (Maintenance Entity Endpoint) is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

A MEP (Maintenance end point) is an inward-facing point at the edge of the domain that defines the boundary and confines CFM messages within these boundaries. Inward facing means that they communicate through the relay function side, not the wire side (connected to the port). See also MIP, Down MEP, and Up MEP.

A MEG End Point (MEP) is a provisioned OAM reference point which can initiate and terminate proactive OAM frames. A MEP can also initiate and react to diagnostic OAM frames. A Point-to-Point EVC has two MEPs, one on each end point of the ME. A Multipoint-to-Multipoint EVC of n UNIs has n MEPs, one on each end point.

MIP

(Maintenance intermediate point) – A point internal to a domain, not at the boundary, that responds to CFM only when triggered by trace route and loopback messages. MIPs forward CFM frames received from MEPs and other MIPs, drop all CFM frames at a lower level, and forward all CFM frames at a higher level, regardless of whether they are received from the relay or wire side.

A MEG Intermediate Point (MIP) is a provisioned OAM reference point that can react to diagnostic OAM frames initiated by MEPs. A MIP does not initiate proactive or diagnostic OAM frames. See also "MEP".

Mirroring

For debugging network problems or monitoring network traffic, the S4224 can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.) Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for **M**ulticast **L**istener **D**iscovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLD is a component of the Internet Protocol Version 6 (IPv6) suite, and is

used by IPv6 routers to discover multicast listeners on a directly attached link (much as IGMP is used in IPv4). MLD is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 similar to IGMPv3. The MLD protocol is described in RFC 3810 which was updated by RFC 4604. Windows Vista and later support MLDv2. FreeBSD 8 supports MLDv2. The Linux kernel has supported MLDv2 since v 2.5.68.

MLD snooping

With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list of ports is created by 'snooping' IPv6 multicast control packets. In IPv6, MLD snooping performs a similar function to the IGMP snooping used in IPv4.

MSTI

An MSTI (**M**ultiple **S**panning **T**ree **I**nstance) is typically one of the uplink ports that connects to one of the gateway devices. Valid MSTI ID values are from 0 through 4094. MSTI information can include VLAN mapping, bridge priority, port priority, and cost. MSTP allows formation of MST regions that can run multiple MST instances (MSTI). Multiple regions and other STP bridges are interconnected using one single common spanning tree (CST). Unlike some proprietary per-VLAN spanning tree implementations, MSTP includes all of its spanning tree information in a single BPDU format. This reduces the number of BPDUs required on a LAN to communicate spanning tree information for each VLAN, and also ensures backward compatibility with RSTP (and effectively, classic STP too). MSTP does this by encoding additional region information after the standard RSTP BPDU as well as a number of MSTI messages (0 to 64 instances; many bridges support fewer). Each of these MSTI configuration messages conveys the spanning tree information for each instance. Each instance can be assigned a number of configured VLANs, and frames (packets) assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. To avoid conveying their entire VLAN to spanning tree mapping in each BPDU, bridges encode an MD5 digest of their VLAN-to-instance table in the MSTP BPDU. This digest is then used by other MSTP bridges, along with other administratively configured values, to determine if the neighboring bridge is in its MST region. See also "CIST".

Multicast address

In IPv6, an identifier for a set of interfaces (typically belonging to different nodes). A packet sent to a multicast address is delivered to all interfaces identified by that address.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

N

NAS

The NAS (**N**etwork **A**ccess **S**erver) is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NDP

(Neighbor Discovery Protocol) - a protocol in the Internet Protocol Suite used with IPv6. NDP operates in the Link Layer and is responsible for address autoconfiguration of nodes, discovery of other nodes on the link, determining the Link Layer addresses of other nodes, duplicate address detection, finding available routers and DNS servers, address prefix discovery, and maintaining reachability information about the paths to other active neighbor nodes per IETF RFC 4861.

Neighbors

Nodes attached to the same link. Per IETF RFC 2461, Neighbor Discovery for IPv6 is done by Sending Router Advertisements and processing Router Solicitation.

NENA

National Emergency Number Association, the body responsible for evolution of public ECS architectures in North America.

NetBIOS

NetBIOS (Network Basic Input/Output System) is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN). The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS (Network File System) allows hosts to mount partitions on a remote system and use them as though they are local file systems. NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NID

Network Interface Devices - a NID is an effective way of providing operational and capital savings to service providers. A NID installs at the customer premise and provides a demarcation point between the service provider and customer's network. NIDs allow for end-to-end Operations, Administration and Maintenance (OAM) functionality for the service provider. The basic functions, such as loopback testing and remote fault isolation, in the NID provide service providers a number of benefits, including: reduced truck rolls, fewer test sets in the field, and increased reliability. The result of this for the service provider is a reduction in OpEx and CapEx while providing a faster return on investment (ROI).

While the operational savings of NIDs can be shown with their features and capabilities for remote troubleshooting, easy installation and SLA monitoring to reduce SLA penalties, it is important for service providers to be aware of the additional revenue streams and services that can be achieved when using a NID at the demarcation point. NIDs have advanced features such as bandwidth allocation, QoS, VLAN and other features that allow the service provider the capability to provide tiered service offerings to customers.

NMS

Network Management System. Contrast "EMS".

NNI

(Network to Network Interface) In carrier Ethernet, the demarcation / peering point between service providers (ENNI) or between service provider internal networks (I-NNI), per MEF 3, 12, 17, 4, 30, 31.

Node

In IPv6, a device that implements IPv6.

Non-revertive mode

In non-revertive mode of unidirectional protection switching operation, in conditions where working traffic is being transmitted via the protection entity, if local protection switching requests have been previously active and now become inactive, a local "do-not-revert state" is entered. Since this state now represents the highest priority local request, it is indicated on the transmitted "request/state" information and maintains the switch, preventing reversion back to the released bridge-selector position in non-revertive mode under no-request conditions. With bidirectional protection switching operation, a local do-not-revert state is entered when there is no higher priority of request received from the far end than that of the do-not-revert state, or when both the local state and far-end state are NR with the requested signal number 1. Generally, Revertive operation is useful when the working transport entity is more optimized or the protection transport entity carries best effort traffic; Non-revertive operation can minimize the number of switching and service outage time. See also "Revertive mode".

NTP

NTP (Network Time Protocol) is a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

OAM

OAM (Operation Administration and Maintenance) protocol is described in ITU-T Y.1731 and is used to implement carrier ethernet functionality. MEP functionality like CC and RDI is based on this. The S4224 provides configuration and monitoring of two types of Ethernet OAM:

- 1) end-to-end service OAM (SOAM) per IEEE 802.1ag and ITU-T Y.1731, to let Ethernet service providers monitor their services proactively, measure end-to-end performance, and guarantee that the customers receive the contracted SLA. Fault monitoring and performance measurement include frame delay, frame delay variation, frame loss and availability.
- 2) single segment Link OAM (LOAM) per IEEE 802.3ah for remote management and fault indication, including remote loopback, dying gasp, and MIB parameter retrieval.

OID

(Object IDentifier) Many standards define certain objects that require unambiguous identification, which can be achieved by 'registration'. Registration is the assignment of an object identifier (OID) to an object in a way which makes the assignment available to interested parties. It is carried out by a registration authority. Registration can be effected by publishing in the standard the names and the corresponding definitions of object. Such a mechanism requires amendment of the standard for each registration, and hence is not appropriate in cases where the registration activity is high. Alternatively, registration can be affected by letting organizations act as registration authorities to perform registration on a flexible basis.

The registration tree is managed in a completely decentralized way (a node gives full power to its children) and it is impossible to be exhaustive (particularly world-wide). The registration tree is defined and managed following the ITU-T X.660 & X.670 Recommendation series (or the ISO/IEC 9834 series of International Standards).

One-step clock

A clock that provides time information using a single event message.

Optional TLVs

An LLDP frame contains multiple TLVs. For some TLVs it is configurable if the S4224 includes the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

Ordinary clock

A clock that has a single Precision Time Protocol port in a domain and maintains the timescale used in the domain. It may serve as a source of time (i.e., be a master clock), or may synchronize to another clock (i.e., be a slave clock). An ordinary clock is a 1588 clock with a single PTP port.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

P

Packet

An IPv6 header plus payload.

Parent clock

The master clock to which a clock is synchronized.

Path MTU

The minimum IPv6 link MTU of all the links in a path between a source node and a destination node.

Path Cost

A path cost value is given to each port. The cost is usually based on 802.1d guidelines. According to the original specification, cost is 1,000 Mbps (1 gigabit per second) divided by the bandwidth of the segment connected to the port. Therefore, a 10 Mbps connection would have a cost of $(1,000/10) = 100$.

A 'path cost' is an administratively assigned value for the contribution of a port to the path cost of paths toward the spanning tree root. A value of '0' assigns the automatically calculated default Path Cost value to the port (the default Path Cost). This complements the object dot1dStpPortPathCost or dot1dStpPortPathCost32, which returns the operational value of the path cost.

Typical STP path costs are shown below for certain data rates.

| <u>Data rate</u> | <u>STP Cost (802.1D-1998)</u> | <u>RSTP Cost (802.1W-2001)</u> |
|------------------|-------------------------------|--------------------------------|
| 4 Mbps | 250 | 5,000,000 |
| 10 Mbps | 100 | 2,000,000 |
| 16 Mbps | 62 | 1,250,000 |
| 100 Mbps | 19 | 200,000 |
| 1 Gbps | 4 | 20,000 |
| 2 Gbps | 3 | 10,000 |
| 10 Gbps | 2 | 2,000 |

The recommended values for any intermediate link speed can be calculated as $20,000,000,000/(\text{Link Speed in Kb/s})$. Limiting the range of the Path Cost parameter to 1-200,000,000 ensures that the accumulated Path Cost cannot exceed 32 bits over a concatenation of 20 hops.

PCP

PCP (Priority Code Point) is a 3-bit field storing the priority level for the 802.1Q frame (also known as User Priority.)

PD

PD (Powered Device) in a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PDU

(Protocol Data Units) 1. Information that is delivered as a unit among peer entities of a network and that may contain control information, address information or data. 2. In a layered system, a unit of data which is specified in a protocol of a given layer and which consists of protocol control information and possibly user data of that layer.

Peer-to-peer transparent clock

A transparent clock that, in addition to providing Precision Time Protocol event transit time information, also provides corrections for the propagation delay of the link connected to the port receiving the PTP event message. In the presence of peer-to-peer transparent clocks, delay measurements between slave clocks and the master clock are performed using the peer-to-peer delay measurement mechanism.

Per flow QoS

The ability to identify a traffic flow, enable rules on how that specific flow should be treated, and then define how the flow should behave when forwarded with other traffic flows. See also "flow".

PHY

PHY (Physical Interface Transceiver) is the device that implements the Ethernet physical layer per IEEE-802.3.

PIC

(Peripheral interface controller) a family of specialized microcontroller chips.

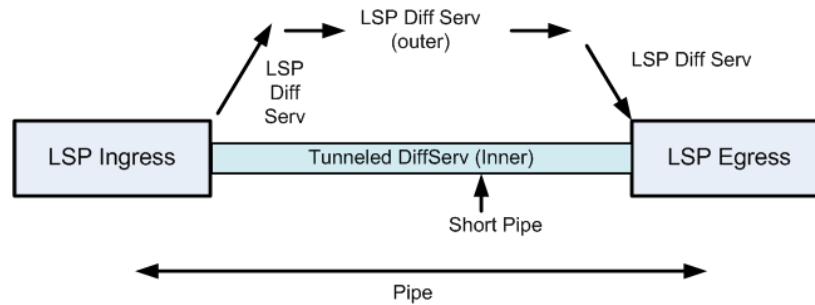
PING

The ping program sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received

the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected. Ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

Pipe Model

One of three different models defined in RFC 3270, and which define, for example, inheritance of TTL and EXP/TC in the label stack during push and pop. TTL inheritance is defined in IETF RFC 4343. See also "Short Pipe Model" and "Uniform Model".



PoE

PoE (Power Over Ethernet) is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

Preferred address

In IPv6, an address assigned to an interface whose use by upper layer protocols is unrestricted. Preferred addresses may be used as the source (or destination) address of packets sent from (or to) the interface.

Preferred lifetime

In IPv6, the length of time that a valid address is preferred (i.e., the time until deprecation). When the preferred lifetime expires, the address becomes deprecated.

Private VLAN

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN (PVLAN).

PSC

Per Hop Behavior Scheduling Class; IETF RFC 3140 defines a binary encoding to uniquely identify PHBs and/or sets of PHBs in protocol messages for cases where it is necessary or desirable to identify a set of PHBs in a protocol message, such as a message negotiating bandwidth management or path selection, especially when such messages pass between management domains.

PTP

PTP (Precision Time Protocol) is a network protocol for synchronizing the clocks of computer systems.

Q

QCE

QCE (QoS Control Entry) describes QoS class associated with a particular QCE ID. There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of four different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL (QoS Control List) is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects. Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL, in SyncE, is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS (Quality of Service) is a method to guarantee a bandwidth relationship between individual applications or protocols. A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required QoS becomes the secret to a successful end-to-end business solution. QoS is the set of techniques to manage network resources.

When discussing QoS features:

- "Packets" carry traffic at Layer 3.
- "Frames" carry traffic at Layer 2 (Layer 2 frames carry Layer 3 packets).
- "Classification" is the selection of traffic to be marked.
- "Marking" (per RFC 2475) is the process of setting a Layer 3 DSCP value of a packet.
- "Policing" is limiting bandwidth used by a flow of traffic; policing can either mark or drop traffic.

R

R-APS

R-APS is an acronym for Ring APS. Per G.8032v1, in ERPS there is a central node called the 'RPL Owner Node' which blocks one of the ports to ensure that there is no loop formed for the Ethernet traffic. The link blocked by the RPL Owner node is called the Ring Protection Link or RPL. The node at the other end of the RPL is known as RPL Neighbour Node. It uses R-APS control messages to coordinate the activities of switching on/off the RPL link.

Any failure along the ring triggers an R-APS(SF) (R-APS signal fail) message along both directions from the nodes adjacent to the failed link after these nodes have blocked the port facing the failed link. On obtaining this message, RPL owner unblocks the RPL port. Note that a single link failure anywhere in the ring ensures a loop free topology.

During the recovery phase when the failed link gets restored, the nodes adjacent to the restored link send R-APS (NR) (R-APS no request) messages. On obtaining this message, the RPL owner blocks the RPL port and then sends a R-APS (NR,RB) (R-APS no request, root blocked) messages. This causes all other nodes other than the RPL Owner in the ring to unblock all of the blocked ports.

This protocol is robust enough to work for unidirectional failure and multiple link failure scenarios in a ring topology. It allows mechanism to force switch (FS) or manual switch (MS) to support field maintenance scenarios.

R-APS virtual channel

The Ring Automatic Protection Switching (R-APS) channel connection between two interconnection nodes of a sub-ring in (an)other Ethernet ring(s) or network(s). Its connection characteristics (e.g., path, performance, etc.) are influenced by the characteristics of the network (e.g., Ethernet ring) providing connectivity between the interconnection nodes. From ITU-T Rec.G.8032/Y.1344 (03/2010).

RARP

RARP (**R**everse **A**ddress **R**esolution **P**rotocol) is a protocol used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS (**R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice) is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI

RDI (Remote Defect Indication) is an OAM function used by a MEP to indicate a defect detected to the remote peer MEP. The IEEE Remote Defect Indication (RDI) is a single bit carried by the CCM. The absence of RDI in a CCM indicates that the transmitting MEP is receiving CCMs from all configured MEPs.

A MEP can use ITU-T ETH-RDI to notify its peer MEPs that it detects a defect condition. ETH-RDI is used only if ETH-CC transmission is enabled. ETH-RDI is used in single-ended fault management and in contributing to far-end performance monitoring. A MEP in a defect condition transmits frames with ETH-RDI information. When a MEP receives frames with ETH-RDI information it determines that its peer MEP has encountered a defect condition.

A MEP, on detecting a defect condition with its peer MEP, sets the RDI field in the CCM frames for the duration of the defect condition. CCM frames are transmitted periodically based on the CCM transmission period when the MEP is enabled for CCM frames transmission. When the defect condition clears, the MEP clears the RDI field in the CCM frames in subsequent transmissions.

Reversion Time (WTR time)

In revertive mode, the Reversion Time is the difference between the repair instant of the original resource and the Reversion Instant.

Revertive Mode

Protection is in revertive mode if, after a resource failure and its subsequent repair, the network automatically reverts to using this initial resource. The protection is in non-revertive mode otherwise. Automatic reversion may include a reversion timer (i.e., the Wait To Restore), which delays the time of reversion after the repair.

In Revertive mode of unidirectional protection switching operation, in conditions where working traffic is being received via the protection entity, if local protection switching requests have been previously active and now become inactive, a local wait-to-restore state is entered. Since this state now represents the highest priority local request, it is indicated on the transmitted "request/state" information and maintains the switch. With bidirectional protection switching, a local wait-to-restore state is entered only when there is no higher priority of request received from the far end than that of the wait-to-restore state. This state normally times out and becomes a no request state after the wait-to-restore timer has expired. The wait-to-restore timer is deactivated earlier if any local request of higher priority pre-empts this state. A switch to the protection entity may be maintained by a local wait-to-restore state or by a remote request (wait-to-restore or other) received via the "request/state" information. So, in a case

where a bidirectional failure for a working entity has occurred and subsequent repair has taken place, the bidirectional reversion back to the working entity does not take place until both wait-to-restore timers at both ends have expired. See also "Non-revertive mode".

Ring MEL

The Maintenance Entity Group (MEG) Level providing a communication channel for ring automatic protection switching (R-APS) information. From ITU-T Rec.G.8032/Y.1344 (03/2010).

Ring Protection Link (RPL)

The ring link that under normal conditions, i.e., without any failure or request, is blocked (at one or both ends) for traffic channel, to prevent the formation of loops. From ITU-T Rec.G.8032/Y.1344 (03/2010).

RPL Neighbour node

The RPL neighbour node, when configured, is an Ethernet ring node adjacent to the RPL that is responsible for blocking its end of the RPL under normal conditions (i.e., the ring is established and no requests are present in the ring) in addition to the block by the RPL owner node. However, it is not responsible for activating the reversion behaviour. From ITU-T Rec.G.8032/Y.1344 (03/2010). Contrast "RPL Owner Node".

RPL Owner node

The RPL owner node is an Ethernet ring node adjacent to the RPL that is responsible for blocking its end of the RPL under normal conditions (i.e., the ring is established and no requests are present in the ring). Furthermore, it is responsible for activating reversion behaviour from protected or manual switch/forced switch (MS/FS) conditions. From ITU-T Rec.G.8032/Y.1344 (03/2010). Contrast "RPL Neighbor Node".

Router

In IPv6, a node that forwards IPv6 packets not explicitly addressed to itself.

Router Port

A port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the **R**apid **S**panning **T**ree **P**rotocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SA

(Source Address); contrast DA.

SAMBA

Samba is a program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.

Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2. Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".

SFP

Small Form Factor Pluggable module (1-4Gbps).

SFP+

Small Form Factor Pluggable Plus module (8-10Gbps).

SHA

SHA (**S**ecure **H**ash **A**lgorithm) is designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

SHA is an authentication protocol; one of two cryptography methods used for S4224 user authentication. SHA-1 is a cryptographic hash function designed by the National Security Agency (NSA) and published by the NIST as a U.S. FIPS standard. SHA-1 is part of many widely accepted security applications and protocols (e.g., TLS, SSL, PGP, SSH, S/MIME, and IPsec). See also "MD5".

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

Short Pipe Model

One of three different models defined in RFC 3270, and which define, for xample, inheritance of TTL and EXP/TC in the label stack during push and pop. TTL inheritance is defined in RFC 4343. See also "Pipe Model" and "Uniform Model".

Site-local Address

An IPv6 addresses for local site only. In IPv6, an address having scope that is limited to the local site.

SMAC

(Source MAC Address) The 12 hex digits of a source MAC address consist of the first/left 6 digits (which should match the vendor of the Ethernet NIC) and the last/right 6 digits which specify the interface serial number for that interface controller vendor. See also "DMAC". The list below identifies some of the blocks of assigned vendor MAC addresses (i.e. the first 3 bytes of a MAC source address).

00000C Cisco
00000E Fujitsu

00000F NeXT
 00001D Cabletron
 000022 Visual Technology
 00002A TRW
 00005A S & Koch
 00005E IANA
 000065 Network General
 00006B MIPS
 000093 Proteon
 08005A IBM
 080067 Comdesign
 080069 Silicon Graphics
 08007C Vitalink TransLAN III
 080080 XIOS
 080086 Imagen/QMS
 080087 Xyplex terminal servers
 080089 Kinetics AppleTalk-Ethernet interface
 080090 Retix Inc Bridges

SMTP

SMTP (Simple Mail Transfer Protocol) is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP (Simple Network Management Protocol) is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP (Simple Network Time Protocol) is a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SOAM

(Service OAM) provides Ethernet Connectivity Fault Management (CFM) per IEEE 802.1AG. Ethernet CFM comprises three protocols that work together to help administrators debug Ethernet networks: continuity check, link trace and loopback protocols. The S4224 supports both Link layer OAM (LOAM, per IEEE 802.3-2005 Clause 57) and Service layer OAM (SOAM, per IEEE 802.1AG and Y.1731). Compare to 'LOAM'.

Solicited-node multicast address

In IPv6, a multicast address to which Neighbor Solicitation messages are sent. The algorithm for computing the address is given in Discovery.

Spanning Tree

The original spanning-tree protocol (STP) was created to prevent broadcast storms and other unwanted side effects of looping. Since, STP has been standardized as the 802.1d specification by the IEEE.

A spanning tree uses a spanning-tree algorithm (STA) to sense that the switch has more than one way to communicate with a node, then determine the best way, and then block out all other paths. The STA also keeps track of the other paths, in case the primary path becomes unavailable.

Each switch is assigned a group of IDs - one for the switch itself and one for each port on the switch.

A switch's bridge ID (BID) is 8 bytes long and contains a bridge priority (2 bytes) along with one of the switch's MAC addresses (6 bytes). Each port ID is 16 bits long with two parts - a 6-bit priority setting and a 10-bit port number. A 'path cost' value is assigned to each port. See also "Path Cost".

SPME

TCM can be supported by the instantiation of a sub-path maintenance element (SPME) that has a 1:1 relationship with the monitored connection. See IETF RFC 6371 section 3.2. The SPME is then monitored using normal label switched path (LSP) monitoring. When an SPME is established between non-adjacent nodes, the edges of the SPME become adjacent at the client sub-layer network and any intermediate node that were previously in between becomes an intermediate node for the SPME. See also "TCM".

SSID

Service **S**et **I**dentifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (Wikipedia).

SSH

SSH (**S**ecure **S**hell) is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM in SyncE is an abbreviation for Synchronization Status Message and contains a QL indication.

SSM

SSM (Source-Specific Multicast) IP version 4 (IPv4) addresses in the 232/8 (232.0.0.0 to 232.255.255.255) range are designated as source-specific multicast (SSM) destination addresses and are reserved for use by source-specific applications and protocols. For IP version 6 (IPv6), the address prefix FF3x::/32 is reserved for source-specific multicast use. IETF RFC 4607 defines an extension to the Internet network service that applies to datagrams sent to SSM addresses and defines the host and router requirements to support this extension.

Source-specific multicast (SSM) is a method of delivering multicast packets in which the only packets that are delivered to a receiver are those originating from a specific source address requested by the receiver. By so limiting the source, SSM reduces demands on the network and improves security. SSM requires that the receiver specify the source address and explicitly excludes the use of the (*,G) join for all multicast groups in RFC 3376, which is possible only in IPv4's IGMPv3 and IPv6's MLDv2.

The burden of source discovery on the network can be significant with a large number of sources. In the SSM model, in addition to the receiver expressing interest in traffic to a multicast address, the receiver expresses interest in receiving traffic from only one specific source sending to that multicast address. This relieves the network of discovering many multicast sources and reduces the amount of multicast routing information that the network must maintain. SSM requires support in last-hop routers and in the receiver's operating system. SSM support is not required in other network components, including routers and even the sending host. Interest in multicast traffic from a specific source is conveyed from hosts to routers using IGMPv3 as specified in RFC 4607. SSM destination addresses must be in the range of 232.0.0.0/8 for IPv4 or FF3x::/96 for IPv6.

SSM identifies a set of multicast hosts not only by group address but also by source. An SSM group, called a 'channel', is identified as (S,G) where S is the source address and G is the group address.

Stateless auto-configuration

A process to get IPv6 addresses from IPv6 standards.

Stateless

A communications protocol that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of requests and responses. A stateless protocol does not require the server to retain session information or status about each communications partner for the duration of multiple requests. An example of a stateless protocol is the Hypertext Transfer Protocol (HTTP) which is the foundation of data communication for the World Wide Web.

The stateless design simplifies the server design because there is no need to dynamically allocate storage to deal with conversations in progress. If a client dies in mid-transaction, no part of the system needs to be responsible for cleaning the present state of the server. A disadvantage of statelessness is that it may be necessary to include additional information in every request, and this extra information will need to be

interpreted by the server. An example of a stateless protocol is HTTP. The protocol provides no means of storing a user's data between requests. As a work-around, HTTP Servers implement various session management methods, typically utilizing a unique identifier in a cookie or parameter that allows the server to track requests originating from the same client. Contrast this with a traditional FTP server that conducts an interactive session with the user. During the session, a user is provided a means to be authenticated and set various variables (working directory, transfer mode), all stored on the server as part of the user's state. From Wikipedia.

STP

Spanning **T**ree **P**rotocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

Sub-ring

An Ethernet ring which is connected to one or more other Ethernet rings or networks through using a pair of interconnection nodes. On their own, the sub-ring links do not form a closed loop. A closed connection of traffic may be formed by the sub-ring links and one or more links that are controlled by another Ethernet ring or network, between interconnection nodes. From ITU-T Rec.G.8032/Y.1344 (03/2010).

Sub-ring link

A span (e.g., link/port) connecting adjacent sub-ring nodes that is under the control of the Ethernet ring protocol control process (ERP control process) of the sub-ring. From ITU-T Rec.G.8032/Y.1344 (03/2010).

Subnet Mask (Address Mask)

A bit mask used to identify which bits in an IP address correspond to the network and subnet portions of the address. Referred to as the 'subnet' mask because the network portion of the address (the network mask) can be determined by the encoding inherent in an IP address.

Synchronized clocks

Two clocks are synchronized to a specified uncertainty when they have the same epoch and their measurements of the time of a single event at an arbitrary time differ by no more than that uncertainty.

T

TACACS+

TACACS+ (**T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem **P**lus) is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag

An optional field in a frame header. In MEF 26 it is the 4-byte field that, when present in an Ethernet frame, appears immediately after the Source Address, or another tag in an Ethernet frame header and which consists of the 2-byte Tag Protocol Identification Field (TPID) which indicates S-Tag or C-Tag, and the 2-byte Tag Control Information field (TCI) which contains the 3-bit Priority Code Point, and the 12-bit VLAN ID field.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP (Transmission Control Protocol) is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers. The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the

packets back into the complete message at the other end. Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

Telnet

TELNET (**TEL**etype **NET**work) is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client. TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

Tentative address

In IPv6, an address whose uniqueness on a link is being verified, prior to its assignment to an interface. A tentative address is not considered assigned to an interface in the usual sense. An interface discards received packets addressed to a tentative address, but accepts Neighbor Discovery packets related to Duplicate Address Detection for the tentative address.

TFTP

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) is a transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

Throttling

An S4224 function used to limit the number of multicast groups to which a switch port can belong.

ToS

ToS (**T**ype **o**f **S**ervice) is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV (**T**ype **L**ength **V**alue). An LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV. For the Type, Length, Value format, LLDP frames are sent by each equipment on each port at a fixed frequency. A frame contains a Link Layer Discovery Protocol Data Unit (LLDPDU) which is a set of type, length, value (TLV) structures. An LLDP frame should start with mandatory TLVs (e.g., Chassis ID, Port ID, and Time to live). These mandatory TLVs are followed by any number of optional TLVs. The frame should end with a special TLV named end of LLDPDU. The IEEE 802.1ab specification contains a description of all of the TLV types.

TKIP

TKIP is an acronym for **T**emporal **K**ey **I**ntegrity **P**rotocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

Transparent clock

A device that measures the time taken for a Precision Time Protocol event message to transit the device and provides this information to clocks receiving this PTP event message.

Two-step clock

A clock that provides time information using the combination of an event message and a subsequent general message.

U

UDP

UDP (**U**ser **D**atagram **P**rotocol) is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers. UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact. Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UNI

(User Network Interface) the physical interface or port that is the demarcation between the customer and the service provider/Cable Operator/Carrier/MSO per MEF 4.

UNI-C

UNI – Customer per MEF 4. A compound architectural component on the Subscriber side of the UNI that represents all the functions required to connect a subscriber to a MEN (per MEF 27).

UNI-N

UNI – Network per MEF 4. A compound functional element used to represent all of the functional elements required to connect a MEN to a MEN subscriber implementing a UNI C. The functional elements within the Customer Edge that supports the MEN Subscriber's technical capabilities and compliance to the UNI specification. A set of one or more functional elements that supports the MEN Service Provider's technical capabilities and compliance to the UNI specification. (Per MEF 27.)

Unicast address

In IPv6, an identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.

Uniform Model

One of three different Diffserv tunneling models defined in RFC 3270, and which define e.g. inheritance of TTL and EXP/TC in the label stack during push and pop. TTL inheritance is defined in RFC 4343. See also "Pipe Model" and "Short Pipe Model".

UPnP

UPnP (**U**niversal **P**lug **a**nd **P**lay). The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.

Upper layer

In IPv6, a protocol layer immediately above IPv6. Examples are transport protocols such as TCP and UDP, control protocols such as ICMP, routing protocols such as OSPF, and internet or lower-layer protocols being "tunneled" over (i.e., encapsulated in) IPv6 such as IPX, AppleTalk, or IPv6 itself.

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

V

Valid IPv6 address

In IPv6, a preferred or deprecated address. A valid address may appear as the source or destination address of a packet, and the internet routing system is expected to deliver packets sent to a valid address to their intended recipients. See the IETF "[Recommendation for IPv6 Address Text Representation](#)" or use a validator for IPv6 address formats such as <http://www.intermapper.com/ipv6validator>.

Valid lifetime

In IPv6, the length of time an address remains in the valid state (i.e., the time until invalidation). The valid lifetime must be greater than or equal to the preferred lifetime. When the valid lifetime expires, the address becomes invalid.

VeriPHY[®]

Cable diagnostics that detect cable conditions such as cable length, opens, shorts, coupling between pairs, and termination status. The VERIPHY trademark was assigned a serial number by the USPTO June 11, 2002 (Type Of Mark: Service Mark). The current federal status of this trademark filing is Cancelled - Section 8.

VLAN

Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

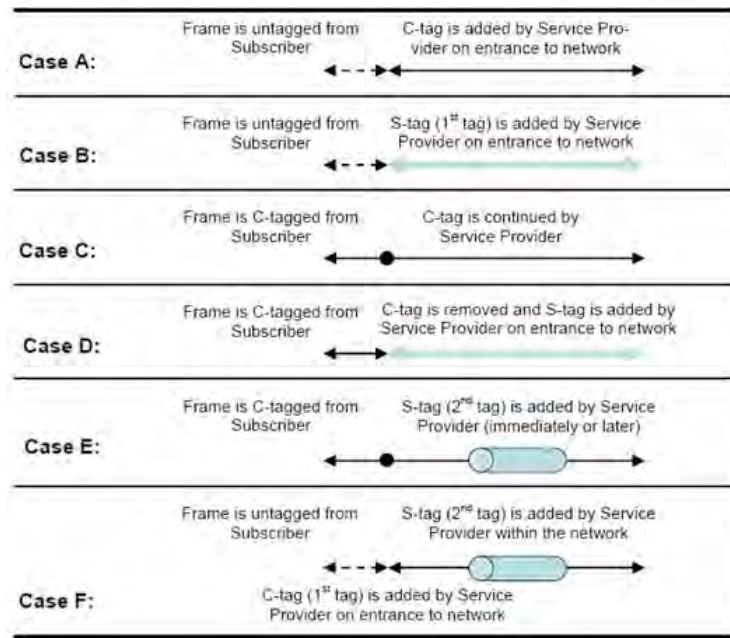
Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

VLAN Tagging

In cases A - D below, a SOAM PDU is initiated by a Customer, and as it flows over the data path it continues to be processed and treated as a SOAM PDU. These frames exist in the OAM Flow Space seen by the Service Provider and the Operator. Thus MEG Levels used at any point can be seen by any other point in the path (subject to [IEEE 802.1ag restrictions on the extent of the MEG Levels). So different parties, such as the Service Provider and Operator, must coordinate the use of all levels that they share.



In Cases E and F above, the SOAM PDUs that were inserted in the un-tagged or single-tagged portions of the path are invisible to all points that are double tagged (since the double-tagged part of the path (the 'tunnel') has hidden the fact that a frame is a SOAM PDU with the addition of a second (outer) tag). These frames do not exist in the OAM Flow Space seen by the Service Provider and the Operator. Within the double-tagging, SOAM PDUs can be inserted and they can use any MEG Level without consideration for the MEG levels used by SOAM PDUs that use single tags.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

VoIP

Voice over Internet Protocol.

VTY

(Virtual Type Terminal) - A **vt**y interface and password must be created in order to enable Telnet access to an IPv6 router. Also Virtual TTY (VTY).

W

WTB

The Wait To Block (WTB) timer is employed by the RPL owner to delay reversion after a forced switch or manual switch has been cleared. From ITU-T Rec.G.8032/Y.1344 (03/2010).

WTR

WTR (Wait To Restore) is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.

Index

| | | | |
|---------------------------------------|----------|---------------------------------------|--------|
| 1:1 port protection scheme | 211 | Loop Protection Configuration | 154 |
| N port protection scheme | 211 | Loopback Configuration | 223 |
| 1+1 port protection scheme | 211 | MAC Address Table Configuration | 259 |
| AAA Configuration | 136 | MAC Table Learning | 260 |
| Access Management Configuration | 63 | MEG levels | 212 |
| ACE Configuration | 101, 111 | Menu system | 13 |
| ACL Configuration | 111 | MEP Configuration | 212 |
| ACL Port Configuration | 101 | MIBs supported | 616 |
| ACL Rate Configuration | 104 | MIP | 212 |
| Aggregation | 141 | MLD Snooping | 185 |
| APS | 206 | Monitor Configuration | 379 |
| ARP Inspection Configuration | 128 | MSTP | 156 |
| Authentication Configuration | 136 | MVR Configuration | 174 |
| Authentication Configuration | 54 | NAS Configuration | 93 |
| Authentication password | 78 | NTP Configuration | 22 |
| change password | 49 | OVC | 307 |
| change privilege level | 51 | Port Aggregation | 141 |
| Configuration Menu | 15 | Port Configuration | 28 |
| configure Privilege Level | 48, 49 | Port Isolation | 275 |
| configure User Name | 48 | Private VLAN Configuration | 273 |
| DHCP Configuration | 32 | Privilege Level Configuration | 51 |
| Down MEP | 212 | Provider Bridging | 271 |
| Dying Gasp | 401 | QoS Configuration | 311 |
| E-Access service | 305 | Read Community | 70 |
| E-LAN | 285 | RMON Configuration | 83 |
| E-LAN service | 304 | RPL Configuration | 251 |
| E-Line | 285 | RSTP | 156 |
| E-Line service | 303 | SNMP Configuration | 65 |
| Engine ID | 71 | SNMP Security Model | 79, 81 |
| ENNI | 305 | SNMP Trap Configuration | 70 |
| EPL service | 303 | SNMP v1 Traps | 69 |
| EP-LAN service | 304 | SNMP v2 Traps | 69 |
| EPS Configuration | 203, 205 | SNMP v3 Traps | 69 |
| EPS Instance Command | 208 | SOAM Configuration | 212 |
| EPS Instance State | 209 | Spanning Tree Configuration | 156 |
| EPS Protection Type | 206 | STP | 156 |
| Ethernet Private Tree service | 305 | STP Bridge Configuration | 157 |
| E-Tree | 285 | Sub-Ring Configuration | 251 |
| EVC Configuration | 290 | SysLog Configuration | 26 |
| EVC types | 285 | Throttling | 179 |
| EVPL service | 303 | Up MEP | 212 |
| Fast Leave | 179 | User Configuration | 48 |
| HTTPS Configuration | 59 | User Privilege Level | 48 |
| LACP Configuration | 144 | VLAN Configuration | 267 |
| Link Aggregation | 141 | VLAN Translation Configuration | 263 |
| Link Speed | 29 | web GUI | 540 |
| LLDP Configuration | 193, 196 | | |



Transition Networks
10900 Red Circle Drive
Minnetonka, MN 55343 USA
Tel: 952-941-7600 or 1-800-526-9267
Fax: 952-941-2322
Copyright © 2014, 2015 Transition Networks.
All rights reserved.

S4xxx Web User Guide, 33595 Rev. B