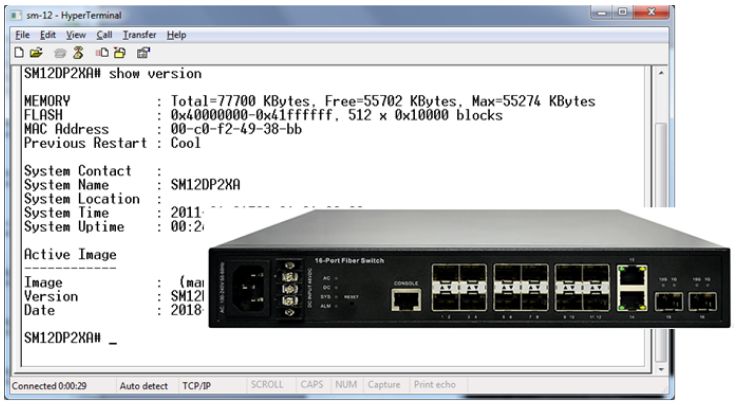


SM12DP2XA

Managed Gigabit Ethernet Fiber Switch

(12) 100/1000Base-X SFP Slots + (2) 1G/10G SFP+ slots

+ (2) 10/100/1000Base-T RJ-45 Ports

CLI Reference

Part Number 33753

Revision E March 2025

Intellectual Property

Warranty

For details on the Lantronix warranty policy, go to http://www.lantronix.com/support/warranty.

Contacts

Lantronix Corporate Headquarters

48 Discovery, Suite 250

Irvine, CA 92618, USA

Toll Free: 800-526-8766

Phone: 949-453-3990

Fax: 949-453-3995

Technical Support

Online: https://www.lantronix.com/technical-support/

Sales Offices

For a current list of our domestic and international sales offices, go to www.lantronix.com/about/contact.

Disclaimer

All information contained herein is provided “AS IS.” Lantronix undertakes no obligation to update the information in this publication. Lantronix does not make, and specifically disclaims, all warranties of any kind (express, implied or otherwise) regarding title, non-infringement, fitness, quality, accuracy, completeness, usefulness, suitability or performance of the information provided herein. Lantronix shall have no liability whatsoever to any user for any damages, losses and causes of action (whether in contract or in tort or otherwise) in connection with the user’s access or usage of any of the information or content contained herein. The information and specifications contained in this document are subject to change without notice.

Revision History

Date	Rev	Description
6/15/20	C	FW v7.10.2544: add Rapid Ring and Interface Config mode commands.
10/3/24	D	FW v7.20.0206: • Add Percepxion and LPM support. • Initial Lantronix rebrand. • Add DHCP per port VLAN. • Add SFTP in CLI. • Add Gateway Address binding interface. • Add 'copy' command merge and replace options. • Add RADIUS and TACACS Key encrypt AES256 on Show Running Config. • Update 'more' command. • Change SNMP mode to disabled by default and change Auth Method default. • Add support for DHCP option 229. • Remove Debug Commands and CLI Command Summary. • Automatically save Config changes to Start-Up Config in Percepxion server. • Fix Cable Diagnostics. See the Release Notes for more information.
3/10/2025	E	FW v7.20.0215 • Add support for MAC Authentication Bypass (MAB) for port level access control. • Update Percepxion description. See the Release Notes for more information.

Contents

1. Introduction

The SM12DP2XA Managed Gigabit Ethernet Fiber Switch is a next-generation Fiber Switch offering full suite of L2 features and additional 10GbE uplink connections. Advanced L3 features such as Static Route deliver better cost performance and lower total cost of ownership in enterprise networks or backbone via fibber or copper connections.

The SM12DP2XA provides 12 GbE SFP ports, 2 RJ45 ports, 2 10GbE SFP+ ports and an RJ45 Console port. It has one AC and one DC power input. The SM12DP2XA provides front panel access to all power, data and management ports in a compact form factor for desktop, wall-mount, or rack-mount installation.

About This Manual

This manual gives specific information on how to operate CLI (Command Line Interface) to manage this switch. The manual is intended for use by network administrators who are responsible for operating and maintaining network equipment. It assumes a strong knowledge of Ethernet switch functions, the RS-232 Console, Internet Protocol (IP), and Telnet Protocol.

Related Manuals

- SM12DP2XA Quick Start Guide, 33750
- SM12DP2XA Install Guide, 33751
- SM12DP2XA Web User Guide, 33752
- SM12DP2XA API User Guide
- Release Notes (version specific)

For Lantronix Drivers, Firmware, Manuals, Product Notifications, Warranty Policy & Procedures, etc. go to the Lantronix Technical Resource Center.

Note: Information in this document is subject to change without notice. Note that this manual provides links to third party web sites for which Lantronix is not responsible.

2. Initial Switch Setup

This chapter describes methods to access the CLI.

Default Configuration Settings

- IP address: 192.168.1.77
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.254
- Username: admin
- Password: admin

To prevent unauthorized access, change the default password on first use and periodically.
Serial settings:

- Baud rate=115200bps
- Data bits=8
- Parity=None
- Stop bits=1
- Flow control=none

Access the CLI through the Console Port

The switch can be accessed and configured using a direct serial connection between the switch and your computer and terminal emulation software on your computer. Use a standard serial cable (RJ-45 to DB9). You will need a USB to serial adapter if your computer doesn't have a serial port.
To access the CLI through the console port:

1. Connect the serial cable to the console port (RJ45) on the switch and to the serial port on the computer (DB9) or use a DB9 to USB adapter if your computer lacks a serial port.
2. Use a terminal emulator program such as PuTTY or Tera Term to start a serial session.
3. Select Serial connection type, select the COM port, and enter the speed.
    a. To find out which COM port to select, go to Device Manager > Ports to view the COM ports in use. (Windows)
4. At the terminal window, enter the factory default username (admin) and password (admin).
5. Perform initial switch configuration using the CLI.

Access the CLI using an SSH or Telnet Connection

The switch can be remotely accessed and configured through the Command Line Interface (CLI) using SSH or Telnet. Use a terminal emulator program such as PuTTY or Tera Term to establish the connection.
Your computer should have an IP address on the same network as the switch and be able to reach the switch's configured management IP address. SSH or Telnet service must be enabled on your switch. Telnet is disabled by default.

Note: *Telnet is not secure and can expose data to potential eavesdroppers. SSH should be used for more secure communication.*

To access the CLI using SSH or Telnet:

1. Launch the terminal emulator program on your computer .
2. Select SSH or Telnet as the session type.
3. Enter the hostname or IP address of the switch. SSH port = 22, Telnet port = 23.
4. At the terminal window, enter the factory default username (admin) and password (admin).
5. Perform switch configuration using the CLI.

Login

Access the CLI through a direct serial connection to the device or using an SSH or Telnet session.
The default username and password are:

- Username: admin
- Password: admin

After you login successfully, the prompt displays as "<sys_name>**#**". The # prompt indicates that you have administrator privilege for setting the managed switch.
If you're logged in as other than the administrator, the prompt displays as "<sys_name>**>**". The > prompt indicates that you have guest privileges and are allowed only a subset of administrator privilege commands. Each CLI command has a particular privilege level.

Example:

```
Username: admin
Password: admin
SM12XPA#
```

You should change the password as soon as possible to prevent unauthorized access.

3. CLI Management

Privilege Levels

Every command has a privilege level (0-15). Users can run a command if the session's privilege level is greater than or equal to the command's privilege level. The session's privilege level initially comes from the login account's privilege level, though it is possible to change the session's privilege level after logging in.

Privilege Level	Types of Commands at this Privilege Level
0	Display basic system information
13	Configure features except for login accounts, the authentication method sequence, multiple logins, and administrator and enable passwords.
15	Configure login accounts, the authentication method sequence, multiple logins, and administrator and enable passwords.

The CLI privilege level and command modes are summarized below.

- The privilege level determines whether or not the user can run the particular commands
- If a user can run a particular command, then the user must run the command in the correct mode.

CLI Command Modes

The CLI is divided into several modes. If a user has enough privilege to run a particular command, you can run the command if in the correct mode. To see the commands of a mode, enter a question mark (**?**) after the system prompt, then all commands will be listed in the screen. The command modes are listed below:

Mode	Prompt	Command Function in this Mode
Exec	<sys_name>#	Display current configuration, diagnostics, maintenance.
Config	<sys_name>(config)#	Configure features other than those below.
Config-if	<sys_name>(config-interface)#	Configure ports.
Config-if-vlan	<sys_name>(config-if-vlan)#	Configure static VLAN.
Config-line	<sys_name>(config-line)#	Line configuration.
Config-impc-profile	<sys_name>(config-impc-profile)#	Configure IPMC Profile.
Config-snmp-host	<sys_name>(config-snmp-host)#	Configure SNMP Server Host.
Config-stp-aggr	<sys_name>(config-stp-aggr)#	Configure STP Aggregation.
Config-dhcp-pool	<sys_name>(config-dhcp-pool)#	DHCP Pool Configuration.
Config-rfc2544-profile	<sys_name>(config-rfc2544-profile)#	RFC2544 Profile Configuration.

Changing Between Command Modes

Each command resides in a corresponding mode and can run only in that mode. If you want to run a particular command, you must change to the appropriate mode. The command modes are organized as a tree, starting in Exec mode. The following table explains how to change from one mode to another.

Exec	--	--
Config	Configure terminal	exit
config-interface	Interface <port-type> <port-type-list>	exit
config-vlan	Interface vlan <vlan_list>	exit

Command Line Controls

To navigate the command line:

Control	Press	Description
more	-	Dash key
next page	space	Space bar

Control	Press	Description
continue	g	g key
quit	^C	Control C
parameters	?	Single Question mark
syntax	??	Two Question marks
available commands in table format	Tab key	Show available commands in tabular format

4. Exec Mode Commands

Exec mode commands are listed with the ? (question mark) command as shown below.

```
SM12DP2XA# ?
CableDiag     Cable Diagnostic keyword
clear         Reset functions
configure     Enter configuration mode
copy          Copy from source to destination
delete        Delete one file in flash: file system
dir           Directory of all files in flash: file system
disable       Turn off privileged commands
do            To run exec commands in config mode
dot1x         IEEE Standard for port-based Network Access Control
enable        Turn on privileged commands
exit          Exit from EXEC mode
firmware      Firmware upgrade/swap
help          Description of the interactive help system
ip            IPv4 commands
ipv6          IPv6 configuration commands
logout        Exit from EXEC mode
more          Display file
no            Negate a command or set its defaults
ping          Send ICMP echo messages
platform      Platform configuration
reload        Reload system.
send          Send a message to other tty lines
show          Show running system information
terminal      Set terminal line parameters
traceroute    traceroute program
SM12DP2XA#
```

CableDiag

Cable Diagnostic keyword. This command runs the built-in Cable Diagnostics. It takes about 5-15 seconds. When completed, the cable diagnostics results display in the cable status table. Note that Cable Diagnostics is only accurate for cables of length 7 -140 meters. The 10 and 100 Mbps ports will be linked down while running Cable Diagnostics. Running Cable Diagnostics on a 10 or 100 Mbps management port will cause the switch to stop responding until the diagnostics complete.

Syntax: CableDiag interface GigabitEthernet <port_type_id>

Parameters:

interface	Interface keyword
GigabitEthernet	1 Gigabit Ethernet Port
<port_type_id>	Port ID in 1/13-14

Example:

```
SM12DP2XA# CableDiag  interface GigabitEthernet 1/13
Starting Cable Diagnostic - Please wait
Interface              Link Status    Test Result    Length
---------------------  -------------  -------------  -------------
GigabitEthernet 1/13    1G             detect error or check cable length is be
tween 7-120 meters
SM12DP2XA# CableDiag  interface GigabitEthernet 1/14
Starting Cable Diagnostic - Please wait
Interface              Link Status    Test Result    Length
---------------------  -------------  -------------  -------------
GigabitEthernet 1/14    Link Down      Abnormal              2(m)
SM12DP2XA#
```

end

Go back to EXEC mode.

Syntax: end

Example:

```
SM12DP2XA(config)# end
SM12DP2XA#
SM12DP2XA(config)# vlan 10
SM12DP2XA(config-if-vlan)# end
SM12DP2XA#
```

Exit

Exit from Config mode back to Exec mode.

Syntax: exit

Parameters: None.

Example:

```
SM12DP2XA# configure terminal
SM12DP2XA(config)# exit
SM12DP2XA#
```

Help

Description of the interactive help system.

Syntax: help

Parameters: None.

Example:

```
SM12DP2XA# help
Help may be requested at any point in a command by entering a question mark '?'.  If nothing
matches, the help list will be empty and you must backup until entering a '?' shows the available
options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and
describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what
arguments match the input(e.g. 'show pr?'.)
SM12DP2XA#
```

logout

Exit from EXEC mode and close the terminal session. You must log back in again.

Syntax: logout

Parameters: none

Example:

```
SM12DP2XA# logout
```

more

Display a file one screen at a time.

Syntax: **more** <path>

Parameters:

<url_file>	File in FLASH or on TFTP server. Syntax: <flash:filename | tftp://server/path-and-filename>. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score(_). The maximum length is 57 and hyphen must not be first character. The file name content that only contains '.' is not allowed.

Example:

```
SM12DP2XA# more flash:test.txt ?
   |       Output modifiers
   <cr>
SM12DP2XA# more flash:test.txt tftp:// ?
                              ^
% Invalid word detected at '^' marker.
SM12DP2XA#
```

5. Clear Commands

Table : clear Commands

access	Access management
access-list	Access list
dot1x	IEEE Standard for port-based Network Access Control
ip	Interface Internet Protocol config commands
ipv6	IPv6 configuration commands
lacp	Clear LACP statistics
lldp	Clears LLDP statistics.
logging	System logging message
mac	MAC Address Table
mvr	Multicast VLAN Registration configuration
port-security	Enable/disable port security globally.
sflow	Statistics flow.
spanning-tree	STP Bridge
statistics	Clear statistics for one or more given interfaces

access

Access management.

Syntax: **clear** access | management | statistics

Parameters: **management** Access management configuration.

statistics Statistics data.

Example:

```
SM12DP2XA# clear access management statistics
SM12DP2XA# show access management statistics


Access Management Statistics:
-----------------------------
HTTP     Receive:          0    Allow:          0    Discard:          0
HTTPS    Receive:          0    Allow:          0    Discard:          0
SNMP     Receive:          0    Allow:          0    Discard:          0
TELNET   Receive:          0    Allow:          0    Discard:          0
SSH      Receive:          0    Allow:          0    Discard:          0
SM12DP2XA#
```

access-list

Access list.

Syntax: **Clear** access-list ace statistics

Parameters:

ace	Access list entry
statistics	Traffic statistics

Example:

```
SM12DP2XA# clear access-list ace statistics
SM12DP2XA# show access-list ace statistics


Switch access-list ace number: 0
SM12DP2XA#
```

dot1x

Clear IEEE Standard for port-based Network Access Control.

Syntax

Clear dot1x statistics

Clear dot1x statistics interface GigabitEthernet < PORT_TYPE_LIST>

Parameters

statistics	Clears the statistics counters
interface	Interface
GigabitEthernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
PORT_TYPE_LIST	Port list in 1/1-14 for Gigabit Ethernet, Port list in 1/1-2 for 10Gigabit Ethernet

EXAMPLE

```
SM12DP2XA# clear dot1x statistics
SM12DP2XA# SM12DP2XA#
```

ip

Clear Interface Internet Protocol config commands.

Syntax

clear ip arp

clear ip dhcp detailed statistics { server | client | snooping | relay | helper | all } [interface (<port_type> [<in_port_list>])]

clear ip dhcp relay statistics

clear ip dhcp server binding <ip>

clear ip dhcp server binding { automatic | manual | expired }

clear ip dhcp server statistics

clear ip dhcp snooping statistics [interface (<port_type> [<in_port_list>])]

clear ip igmp snooping [vlan <v_vlan_list>] statistics

clear ip statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

Parameters

arp	Clear ARP cache
dhcp	Dynamic Host Configuration Protocol
igmp	Internet Group Management Protocol
statistics	Traffic statistics
relay	DHCP relay agent configuration
snooping	DHCP snooping
interface	Select an interface to configure
GigabitEthernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
vlan	IPv4 traffic interface
<vlan_list>	VLAN identifier(s): VID

EXAMPLE

```
SM12DP2XA# clear ip arp
SM12DP2XA# clear ip statistics
SM12DP2XA#
```

ipv6

Clear IPv6 configuration commands.

Syntax

clear ipv6 mld snooping [vlan <v_vlan_list>] statistics

clear ipv6 neighbors

clear ipv6 statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

Parameters

mld	Multicasat Listener Discovery
neighbor	Ipv6 neighbors
statistics	Traffic statistics
snooping	Snooping MLD
statistics	Running MLD snooping counters
vlan	Ipv6 interface traffic
<vlan_list>	VLAN identifier(s): VID
icmp	IPv6 ICMP traffic
icmp-msg	IPv6 ICMP traffic for designated message type
interface	Select an interface to configure
system	IPv6 system traffic
< 0~255>	ICMP message type ranges from 0 to 255

EXAMPLE

```
SM12DP2XA# clear ipv6 mld snooping vlan 3 statistics
SM12DP2XA# clear ipv6 neighbors
SM12DP2XA# clear ipv6 statistics system icmp icmp-msg 2
SM12DP2XA#
```

lacp

Clear LACP statistics

Syntax **Clear lacp** statistics

Parameters

statistics	Clear all LACP statistics

EXAMPLE

```
SM12DP2XA# clear lacp statistics
SM12DP2XA#
```

lldp

Clear LLDP statistics.

Syntax

Clear lldp statistics

Clear lldp statistics| begin | exclude | include >< LINE >

Parameters

statistics Clears LLDP statistics.

EXAMPLE

```
SM12DP2XA# clear lldp statistics ?
    |           Output modifiers
    global       Clear global counters
    interface    Interface keyword.
    <cr>
SM12DP2XA# clear lldp statistics <tab>
global     interface  |         <cr>
SM12DP2XA# clear lldp statistics
SM12DP2XA#
```

logging

Clear Syslog.

Syntax

clear logging [info] [warning] [error] [switch <switch_list>]

Parameters

alert crit debug emerg error flash info notice warning

EXAMPLE

```
SM12DP2XA# clear logging ?
    alert      Severity 1: Action must be taken immediately
    crit       Severity 2: Critical conditions
    debug      Severity 7: Debug-level messages
    emerg      Severity 0: System is unusable
    error      Severity 3: Error conditions
    flash      Clear all logging messages on Flash
    info       Severity 6: Informational messages
    notice     Severity 5: Normal but significant condition
    warning    Severity 4: Warning conditions
SM12DP2XA# clear logging <tab>
alert    crit     debug    emerg    error    flash   info     notice   warning
<cr>
SM12DP2XA# clear logging info error warning
SM12DP2XA#
```

mac

Clear MAC Address Table.

Syntax

Clear mac address-table

Parameters

address-table Flush MAC Address table.

EXAMPLE

```
SM12DP2XA# clear mac address-table
SM12DP2XA#
```

mvr

Clear Multicast VLAN Registration configuration.

Syntax

clear mvr [vlan <v_vlan_list> | name <mvr_name>] statistics

Parameters

name	MVR multicast name
statistics	Running MVR protocol counters
vlan	MVR multicast vlan
< word16>	MVR multicast VLAN name
<vlan_list>	MVR multicast VLAN list

EXAMPLE

```
SM12DP2XA# clear mvr ?
    name          MVR multicast name
    statistics    Running MVR protocol counters
    vlan          MVR multicast vlan
SM12DP2XA# clear mvr name ?
    <word16>    MVR multicast VLAN name
SM12DP2XA# clear mvr statistics ?
    <cr>
SM12DP2XA# clear mvr vlan ?
    <vlan_list>    MVR multicast VLAN list
SM12DP2XA# clear mvr vlan 25 statistics
SM12DP2XA#
```

port-security

Clear port security.

Syntax

clear port-security sticky { All | interface (<port_type> [<plist>]) }

Parameters

sticky	port security sticky function per interface
All	clear all sticky mac at all ports
interface	Choose port
*	All switches or All ports
GigabitEthernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-2
<cr>	

EXAMPLE

```
SM12DP2XA# clear port-security?
    port-security    Enable/disable port security globally.
SM12DP2XA# clear port-security ?
    sticky    port security sticky function per interface.
SM12DP2XA# clear port-security sticky ?
    All         clear all sticky mac at all ports
    interface    Choose port
SM12DP2XA# clear port-security sticky interface ?
    *                  All switches or All ports
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
SM12DP2XA# clear port-security sticky interface 10GigabitEthernet ?
    <port_type_list>    Port list in 1/1-2
SM12DP2XA# clear port-security sticky interface 10GigabitEthernet 1/10 ?
% No such interface: 10GigabitEthernet 1/10
SM12DP2XA# clear port-security sticky interface 10GigabitEthernet 1/1
SM12DP2XA# clear port-security sticky all
SM12DP2XA#
```

sflow

Clear Statistics flow.

Syntax

clear sflow statistics { receiver [<receiver_index_list>] | samplers [interface [<samplers_list>] (<port_type> [<v_port_type_list>])] }

Parameters

receiver	Clear statistics for receiver.
samplers	Clear statistics for samplers.
<cr>	
interface	Clear statistics for a specific interface or interfaces.
*	All switches or All ports
GigabitEthernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14

EXAMPLE

```
SM12DP2XA# clear sflow statistics ?
    receiver    Clear statistics for receiver.
    samplers    Clear statistics for samplers.
SM12DP2XA# clear sflow statistics receiver ?
    <cr>
SM12DP2XA# clear sflow statistics samplers ?
    interface    Clear statistics for a specific interface or interfaces.
    <cr>
SM12DP2XA# clear sflow statistics samplers interface ?
    *                  All switches or All ports
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
SM12DP2XA# clear sflow statistics samplers interface GigabitEthernet ?
    <port_type_list>    Port list in 1/1-14
SM12DP2XA# clear sflow statistics samplers interface GigabitEthernet 1/1
SM12DP2XA#
```

spanning-tree

Clear STP Bridge.

Syntax

clear spanning-tree { { statistics [interface (<port_type> [<v_port_type_list>])] } | { detected-protocols [interface (<port_type> [<v_port_type_list_1>])] } }

Parameters

detected-protocols	Set the STP migration check
statistics	STP statistics
interface	Choose port
<port_type>	GigabitEthernet
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet

EXAMPLE

```
SM12DP2XA# clear spanning-tree ?
    detected-protocols    Set the STP migration check
    statistics            STP statistics
SM12DP2XA# clear spanning-tree <tab>
detected-protocols  statistics
SM12DP2XA# clear spanning-tree detected-protocols ?
    interface    Choose port
    <cr>
SM12DP2XA# clear spanning-tree detected-protocols interface ?
    *                  All switches or All ports
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
SM12DP2XA# clear spanning-tree statistics ?
    interface    Choose port
    <cr>
SM12DP2XA# clear spanning-tree statistics interface ?
    *                  All switches or All ports
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
SM12DP2XA# clear spanning-tree statistics interface *
SM12DP2XA#
```

statistics

Clear statistics for one or more given interfaces.

Syntax

clear statistics interface <port_type> <port_type_list>

clear statistics <port_type> <port_type_list>

Parameters

<port_type>	GigabitEthernet
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet

EXAMPLE

```
SM12DP2XA# clear statistics ?
    *                   All switches or All ports
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
    interface           Interface
SM12DP2XA# clear statistics interface ?
    *                   All switches or All ports
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
SM12DP2XA# clear statistics interface 10GigabitEthernet ?
    <port_type_list>    Port list in 1/1-2
SM12DP2XA# clear statistics interface 10GigabitEthernet 1/1
SM12DP2XA#
```

6. Config Mode Commands

To enter Config mode from Exec mode enter:

```
SM24DP4XA# configure terminal
SM24DP4XA(config)#
```

Table : Config Mode Commands

terminal	Enter Config mode from Exec mode.
aaa	Authentication, Authorization and Accounting
access	Access management
access-list	Access list
aggregation	Aggregation mode
banner	Define a login banner
clock	Configure time-of-day clock
command-history-log	Enable to Save Command Histry to Flash
default	Set a command to its defaults
dms	Enter DMS Modes
do	To run exec commands in config mode
dot1x	IEEE Standard for port-based Network Access Control
enable	Modify enable password parameters
end	Go back to EXEC mode
event	Trap event severity level
exec-timeout	Set exec-timeout autologout period
exit	Exit from current mode
gvrp	Enable GVRP feature
help	Description of the interactive help system
hostname	Set system's network name
interface	Select an interface to configure
ip	Internet Protocol
ipmc	IPv4/IPv6 multicast configuration
ipv6	IPv6 configuration commands
lacp	LACP settings
line	Configure a terminal line
lldp	LLDP configurations.
logging	System logging message

loop-protect	Loop protection configuration
mac	MAC table entries/configuration
map-api-key	Set Google Maps key string
monitor	Monitoring different system events
mvr	Multicast VLAN Registration configuration
no	Negate a command or set its defaults
ntp	Configure NTP
percepxion	Configure Percepxion
port-security	Enable/disable port security globally.
privilege	Command privilege parameters
qos	Quality of Service
radius-server	Configure RADIUS
rapid-ring	Set Rapid Ring parameters
rmon	Remote Monitoring
sflow	Statistics flow.
smtp	Set email information
snmp-server	Set SNMP server's configurations
spanning-tree	Spanning Tree protocol
system	Set Board Configuration
tacacs-server	Configure TACACS+
tzidx	Configure timezone city/area
udld	Enable UDLD in aggressive or normal mode and set the configurable message timer on all fiber-optic ports.
upnp	Set UPnP configuration
username	Establish User Name Authentication
vlan	VLAN commands
voice	Voice appliance attributes
web	Web

aaa

Configure Authentication, Authorization and Accounting. You can use RADIUS or TACACS+ for authentication.

Syntax

aaa accounting { console | telnet | ssh } tacacs { [commands <priv_lvl>] [exec] }*1

aaa accounting { http | https } tacacs [exec]

aaa authentication login { console | telnet | ssh | https } { { local | radius | tacacs } [{ local | radius | tacacs } [{ local | radius | tacacs }]] } [fallback]

aaa authentication login { http } { { redirect | local | radius | tacacs } [{ redirect | local | radius | tacacs } [{ redirect | local | radius | tacacs } [{ redirect | local | radius | tacacs }]]] } [fallback]

aaa authorization { console | telnet | ssh } tacacs commands <priv_lvl> [config-commands] [fallback]

aaa authorization { http | https } tacacs [fallback]

Parameters

accounting	Accounting
authentication	Authentication
authorization	Authorization
login	Login
console	Configure Console command accounting
http	Configure HTTP command accounting
https	Configure HTTPS command accounting
ssh	Configure SSH command accounting
telnet	Configure Telnet command accounting
local	Use local database for authentication
radius	Use RADIUS for authentication
tacacs	Use TACACS+ for authentication
fallback	Configure local authentication fallback
console	Configure Console authentication
http	Configure HTTP authentication
https	Configure HTTPS authentication
ssh	Configure SSH authentication
telnet	Configure Telnet authentication
commands	Enable command accounting
<0-15>	Command privilege level. Commands equal and above this level are accounted
exec	Enable EXEC accounting
console	Configure Console command authorization
http	Configure HTTP command authorization

ssh	Configure SSH command authorization
telnet	Configure Telnet command authorization
config-commands	Include configuration commands
fallback	Configure authorization fallback mode
redirect	Secure HTTP web redirection

EXAMPLE

```
SM12DP2XA(config)# aaa accounting console tacacs commands 13 exec
SM12DP2XA(config)# aaa authentication login console local local fallback
SM12DP2XA(config)# aaa authorization console tacacs commands 0 config-commands fallback
SM12DP2XA(config)# aaa authentication login http local redirect
SM12DP2XA(config)#
```

access

Configure Access management via the web, SNMP, telnet, or all.

Syntax

access management

access management <access_id> <access_vid> <start_addr> [to <end_addr>] { [web] [snmp] [telnet] | all }

Parameters

management	Access management configuration
< 1-16>	ID of access management entry
< 1-4094>	The VLAN ID for the access management entry
< ipv4_addr>	Start IPv4 address
< ipv6_addr>	Start IPv6 address
all	All services
snmp	SNMP service
telnet	TELNET/SSH service
to	End address of the range
web	Web service

EXAMPLE

```
SM12DP2XA(config)# access management 1 10 192.168.1.30 all
SM12DP2XA(config)# access management 1 200  192.168.1.77 snmp telnet web
SM12DP2XA(config)#
```

Access-list

These commands configure the Access Control List (ACL), which is made up of the ACEs defined on this switch..

The maximum number of ACEs is 512 on each switch.

An **ACL** (Access Control List) 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.

An **ACE** (Access Control Entry) describes 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.

Table : Configure access-list Commands

Command	Function
ace	Access list entry
rate-limiter	Rate limiter

ace

Configure Access list entry.

Syntax

access-list ace [update] <ace_id> [next { <ace_id_next> | last }] [ingress { switch <ingress_switch_id> | switchport { <ingress_switch_port_id> | <ingress_switch_port_list> } | interface { <port_type> <ingress_port_id> | (<port_type> [<ingress_port_list>]) } | any }] [policy <policy> [policy-bitmask <policy_bitmask>]] [tag { tagged | untagged | any }] [vid { <vid> | any }] [tag-priority { <tag_priority> | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7 | any }] [dmac-type { unicast | multicast | broadcast | any }] [frame-type { any | etype [etype-value { <etype_value> | any }] [smac { <etype_smac> | any }] [dmac { <etype_dmac> | any }] | arp [sip { <arp_sip> | any }] [dip { <arp_dip> | any }] [smac { <arp_smac> | any }] [arp-opcode { arp | rarp | other | any }] [arp-flag [arp-request { <arp_flag_request> | any }] [arp-smac { <arp_flag_smac> | any }] [arp-tmac { <arp_flag_tmac> | any }] [arp-len { <arp_flag_len> | any }] [arp-ip { <arp_flag_ip> | any }] [arp-ether { <arp_flag_ether> | any }]] | ipv4 [sip { <sipv4> | any }] [dip { <dipv4> | any }] [ip-protocol { <ipv4_protocol> | any }] [ip-flag [ip-ttl { <ip_flag_ttl> | any }] [ip-options { <ip_flag_options> | any }] [ip-fragment { <ip_flag_fragment> | any }]] | ipv4-icmp [sip { <sipv4_icmp> | any }] [dip { <dipv4_icmp> | any }] [icmp -type { <icmpv4_type> | any }] [icmp-code { <icmpv4_code> | any }] [ip-flag [ip-ttl { <ip_flag_icmp_ttl> | any }] [ip-options { <ip_flag_icmp_options> | any }] [ip-fragment { <ip_flag_icmp_fragment> | any }]] | ipv4-udp [sip { < sipv4_udp> | any }] [dip { <dipv4_udp> | any }] [sport { <sportv4_udp_start> [to <sportv4_udp_end>] | any }] [dport { <dportv4_udp_start> [to <dportv4_udp_end>] | any }] [ip-flag [ip-ttl { <ip_flag_udp_ttl> | any }] [ip-options { <ip_flag_udp_options> | any }] [ip-fragment { <ip_flag_udp_fragment> | any }]] | ipv4-tcp [sip { <sipv4_tcp> | any }] [dip { <dipv4_tcp> | any }] [sport { <sportv4_tcp_start> [to <sportv4_tcp_end>] | any }] [dport { <dport

v4_tcp_start> [to <dportv4_tcp_end>] | any }] [ip-flag [ip-ttl { <ip_flag_tcp_ttl> | any }] [ip-options { <ip_flag_tcp_options> | any }] [ip-fragment { <ip_flag_tcp_fragment> | any }]] [tcp-flag [tcp-fin { <tcpv4_flag_fin> | any }] [tcp-syn { <tcpv4_flag_syn> | any }] [tcp-rst { <tcpv4_flag_rst> | any }] [tcp-psh { <tcpv4_flag_psh> | any }] [tcp-ack { <tcpv4_flag_ack> | any }] [tcp-urg { <tcpv4_flag_urg> | any }]] | ipv6 [next-header { <next_header> | any }] [sip { <sipv6> [sip-bitmask <sipv6_bitmask>] | any }] [hop-limit { <hop_limit> | any }] | ipv6-icmp [sip { <sipv6_icmp> [sip-bitmask <sipv6_bitmask_icmp>] | any }] [icmp-type { <icmpv6_type> | any }] [icmp-code { <icmpv6_code> | any }] [hop-limit { <hop_limit_icmp> | any }] | ipv6-udp [sip {<sipv6_udp> [sip-bitmask <sipv6_bitmask_udp>] | any }] [sport { <sportv6_udp_start> [to <sportv6_udp_end>] | any }] [dport { <dportv6_udp_start> [to <dportv6_udp_end>] | any }] [hop-limit { <hop_limit_udp> | any }] | ipv6-tcp [sip { <sipv6_tcp> [sip-bitmask <sipv6_bitmask_tcp>] | any }] [sport { <sportv6_tcp_start> [to <sportv6_tcp_end>] | any }] [dport { <dportv6_tcp_start> [to <dportv6_tcp_end>] | any }] [hop-limit { <hop_limit_tcp> | any }] [tcp-flag [tcp-fin { <tcpv6_flag_fin> | any }] [tcp-syn { <tcpv6_flag_syn> | any}] [tcp-rst { <tcpv6_flag_rst> | any }] [tcp-psh { <tcpv6_flag_psh> | any }] [tcp-ack { <tcpv6_flag_ack> | any }] [tcp-urg { <tcpv6_flag_urg> | any }]] }] [action { permit | deny | filter { switchport <filter_switch_port_list> | interface (<port_type> [<fliter_port_list>]) } }] [rate-limiter { <rate_limiter_id> | disable }] [evc-policer { <evc_policer_id> | disable }] [mirror [disable]] [logging [disable]] [shutdown [disable]] [lookup-second [disable]] [redirect { switchport { <redirect_switch_port_id> | <redirect_switch_port_list> } | interface { <port_type> <redirect_port_id> | (<port_type> [<redirect_port_list>]) } | disable }]

Parameters

ace	Access list entry
<1-512>	ACE ID
update	Update an existing ACE
action	Access list action
dmac-type	The type of destination MAC address
frametype	Frame type
ingress	Ingress
logging	Logging frame information
mirror	Mirror frame to destination mirror port
next	insert the current ACE before the next ACE ID
policy	Policy
rate-limiter	Rate limiter
redirect	Redirect frame to specific port
shutdown	Shutdown incoming port
tag	Tag
tag-priority	Tag priority
vid	VID field

deny	Deny
filter	Filter
permit	Permit
any	Don't-care the type of destination MAC address
broadcast	Broadcast destination MAC address
multicast	Multicast destination MAC address
unicast	Unicast destination MAC address
any	Don't-care the frame type
arp	Frame type of ARP
etype	Frame type of etype
ipv4	Frame type of IPv4
ipv4-icmp	Frame type of IPv4 ICMP
ipv4-tcp	Frame type of IPv4 TCP
ipv4-udp	Frame type of IPv4 TCP
ipv6	Frame type of IPv4
ipv6-icmp	Frame type of IPv6 ICMP
ipv6-tcp	Frame type of IPv6 TCP
ipv6-udp	Frame type of IPv6 UDP
interface	Select an interface to configure
<port_type>	* or Gigabitethernet
*	All switches or All ports
Gigabitethernet	1 Gigabit Ethernet port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_id>	Port ID in the format of switch-no/port-no ex, 1/1-14 for Gigabitethernet, 1/1-2 for 10Gigabitethernet
<port_type>	* or Gigabitethernet
*	All Switches or All ports
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet
any	Don't-care the ingress interface
<0-255>	Policy ID
policy-bitmask	The bitmask for policy ID
<0x0-0xFF>	The value of policy bitmask
<1-4095>	The value of VID field
<0-7>	The value of tag priority

EXAMPLE

```
SM12DP2XA(config)# access-list ?
    ace            Access list entry
```

```
    rate-limiter    Rate limiter
SM12DP2XA(config)# access-list ace ?
    <1-512>    ACE ID
    update     Update an existing ACE
SM12DP2XA(config)# $-list ace 1 action filter interface GigabitEthernet 1/2 *
SM12DP2XA(config)# $GigabitEthernet 1/2 policy 1 rate-limiter 1 ingress any
SM12DP2XA(config)#
```

rate-limiter

Rate limiter.

Syntax

access-list rate-limiter [<rate_limiter_list>] { pps <pps_rate> | 10pps <pps10_rate> | 100pps <pps100_rate> | 25kbps <kpbs25_rate> | 100kbps <kpbs100_rate> }

Parameters

10pps	10 packets per second
25kbps	25k bits per second
<1~16>	Rate limiter ID
<0-500000>	Rate value (10pps)
<0-400000>	Rate value (25kbps)

EXAMPLE

```
SM12DP2XA(config)# access-list rate-limiter 10pps 3333
SM12DP2XA(config)# access-list rate-limiter 1 25kbps 6000
SM12DP2XA(config)#
```

aggregation

Configure Aggregation mode. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports.

Syntax

aggregation mode { [smac] [dmac] [ip] [port] }*1

Parameters

mode	Traffic distribution mode
dmac	Destination MAC affects the distribution
ip	IP address affects the distribution
port	IP port affects the distribution
smac	Source MAC affects the distribution

EXAMPLE

```
SM12DP2XA(config)# aggregation mode dmac ip port smac
SM12DP2XA(config)#
```

banner

Define a login banner or Message of the Day banner.

Syntax

banner [motd] <banner>

banner exec <banner>

banner login <banner>

Parameters

<line>	c banner-text c, where 'c' is a delimiting character
exec	Set EXEC process creation banner
login	Set login banner
motd	Set Message of the Day banner

EXAMPLE

```
SM12DP2XA(config)# banner exec bannerText-1
Enter TEXT message.  End with the character 'b'.
Welcome!Banner b
SM12DP2XA(config)#
```

clock

Configure clock date and time-of-day, timezone, and daylight savings time.

Syntax

clock set <icliDateWord> { <icliTimeWord24> | <icliTimeWord12> { AM | PM } }

clock summer-time <word16> date [<start_month_var> <start_date_var> <start_year_var> <start_hour_var> <end_month_var> <end_date_var> <end_year_var> <end_hour_var> [<offset_var>]]

clock summer-time <word16> recurring [<start_week_var> <start_day_var> <start_month_var> <start_hour_var> <end_week_var> <end_day_var> <end_month_var> <end_hour_var> [<offset_var>]]

clock timezone <word_var> <hour_var> [<minute_var> [<subtype_var>]]

Parameters

set	set clock
summer-time	Configure summer (daylight savings) time
timezone	Configure time zone
<word10>	yyyy/mm/dd
<word8>	hh:mm:ss
<word16>	name of time zone in summer
date	Configure absolute summer time
recurring	Configure recurring summer time
<2000-2097>	Year to start
hh:mm	Time to start (hh:mm)
<1-12>	Month to end
<1-31>	Date to end
<2000-2097>	Year to end
hh:mm	Time to end (hh:mm)
<-59-59>	Minutes offset from UTC
<1-5>	Week number to start
<1-7>	Weekday to start
<1-12>	Month to start

EXAMPLE 1

```
SM12DP2XA(config)# clock set 2021/02/10 17:23:31
2021-02-10T17:23:31+00:00
SM12DP2XA(config)# clock summer-time CdtSummer date 5 31 2021 12:00 9 15 2021 11:59 60
SM12DP2XA(config)# clock timezone Chicago -9 0 3
SM12DP2XA(config)# do show clock
System Time     : 2021-02-10T08:32:37-09:00
```

```
SM12DP2XA(config)#
```

Message: *Network error: Software caused connection abort*

command-history-log

Enable saving Command History to Flash.

Syntax

command-history-log <cr>

Parameters

None.

EXAMPLE

```
SM12DP2XA(config)# command-history-log
SM12DP2XA(config)# exit
SM12DP2XA# show command-history-log status
The status of termal for Command History Feature : Enable
SM12DP2XA#
```

default

Set access-list rate-limiter to its defaults.

Syntax

default access-list rate-limiter [<rate_limiter_list>]

Parameters

access-list	Access list
rate-limiter	Rate limiter
<1~16>	Rate limiter ID

EXAMPLE

```
SM12DP2XA(config)# default access-list rate-limiter 1
SM12DP2XA(config)# default access-list rate-limiter 99 ?
                                                    ^
% Invalid word detected at '^' marker.


SM12DP2XA(config)# default  access-list rate-limiter 9
SM12DP2XA(config)#
```

dms

Set DMS modes. The built-in Device Management System (DMS) lets you manage connected devices.
This command lets you enable or disable the DMS function, or select a priority (e.g., “high” to make this device the Master (Controller) switch).

Syntax

dms service-mode { disabled | enabled [priority { high | mid | low | non }] }

Parameters

service-mode	DMS mode (disabled, enabled, high-priority)
disabled	DMS mode disabled
enabled	DMS mode enabled
priority	DMS priority. You can choose the priority to change the dominant status of the switch.
high	DMS priority is highest priority; this switch will become the Master (Controller) switch.
low	DMS priority is lowest priority
mid	DMS priority is mid-level priority
non	DMS priority is none; this switch will never become the Master (Controller) switch.

EXAMPLE

```
SM12DP2XA(config)# dms service-mode enabled priority high
SM12DP2XA(config)# do show dms
DMS Controller Capability : On
Discovery : Arp->On, UPNP->On, NBNS->On, LLDP->On, Onvif->On, Bonjour->On
DMS total device: 2

======= DMS Entry Information Start ============================
(001),MAC(00-c0-f2-49-38-dd),PA_MAC(00-00-00-00-00-00),port(0),p_port(0),C_IP(19
2.168.1.77),C_sub(255.255.255.0),C_gw(192.168.1.254),http_port(80),IP1(192.168.1
.77),IP2(169.254.176.71),IP1_U(3),UM(0),vid(1),prio(99),manufacturers( SM12DP2XA
),d_name(SM12DP2XA),type(1001)(16),status(1),PoE(NoN),group(0)(0),app_fw(0)(0)(0
)(0),time(63172)

(002),MAC(00-1b-11-b2-6d-4b),PA_MAC(00-c0-f2-49-38-dd),port(13),p_port(0),up_lin
k_MAC(00-00-00-00-00-00),up_link_port(0),C_IP(192.168.1.99),C_sub(0.0.0.0),C_gw(
0.0.0.0),http_port(80),IP1(192.168.1.99),IP2(0.0.0.0),IP1_U(2),UM(0),vid(1),prio
(99),manufacturers( ),d_name(Dome camera1),auth(/),type(2001)(0),status(1)(0)(0)
,PoE(NoN),account(),pwd(),media(),profile(),strim(),info/auth(0/0),group(0)(0)(1
),app_fw(0)(0)(0)(0),ver(),time(63160)

======= DMS Entry Information end ============================

======= DMS Grouping Information start ============================
Grouping Entry Cnt(0)
======= DMS Grouping Information end ============================
```

do

To run Exec mode commands in Config mode.

Syntax

do < LINE >{[< LINE >]}

Parameters

<LINE> Exec Command

<cr>

EXAMPLE

```
SM12DP2XA(config)# do ?
    <line>    Exec Command
SM12DP2XA(config)# do show vlan
VLAN  Name                            Interfaces
----  --------------------------------  ----------
1     default                         Gi 1/1-14 10G 1/1-2


SM12DP2XA(config)# do show ip interface brief
Vlan Address             Method   Status
---- ------------------- -------- ------
   1 192.168.1.77/24      Manual   UP
SM12DP2XA(config)#
```

dot1x

802.1X is the IEEE Standard for port-based Network Access Control. This command lets you configure the Network Access Server (NAS) parameters. A NAS server can be used to connect users to a variety of resources including Internet access, conference calls, printing documents on shared printers, or by simply logging on to the Internet. 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.

Syntax

dot1x authentication timer inactivity <v_10_to_100000>

dot1x authentication timer re-authenticate <v_1_to_3600>

dot1x feature { [guest-vlan] [radius-qos] [radius-vlan] }*1

dot1x guest-vlan <value>

dot1x guest-vlan supplicant

dot1x max-reauth-req <value>

dot1x re-authentication

dot1x system-auth-control

dot1x timeout quiet-period <v_10_to_1000000>

dot1x timeout tx-period <v_1_to_65535>

Parameters

authentication	Authentication
feature	Globally enables/disables a dot1x feature functionality
guest-vlan	Guest VLAN
max-reauth-req	Guest VLAN ID used when entering the Guest VLAN.
re-authentication	Set Re-authentication state
system-auth-control	Set the global NAS state
timeout	timeout
timer	timer
inactivity	Time in seconds between check for activity on successfully authenticated MAC addresses.
re-authenticate	The time period between re-authentication attempts in seconds
<10-1000000>	seconds
<1-3600>	seconds
guest-vlan	Globally enables/disables state of guest-vlan
radius-qos	Globally enables/disables state of RADIUS-assigned QoS.
radius-vlan	Globally enables/disables state of RADIUS-assigned VLAN.
<1-4095>	The number of times a Request Identity EAPOL frame is sent without response before considering entering the Guest VLAN.

supplicant	The switch remembers if an EAPOL frame was 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, 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..
<1-255>	number of times to try to re-authenticate.
quiet-period	Time (secs) before a MAC-address that failed authent gets a new authent chance.
tx-period	the time between EAPOL retransmissions.
<10-1000000>	seconds
<1-65535>	seconds

EXAMPLE

```
SM12DP2XA(config)# dot1x authentication timer inactivity 500000
SM12DP2XA(config)# dot1x guest-vlan 1
SM12DP2XA(config)# dot1x feature guest-vlan radius-qos
SM12DP2XA(config)# dot1x max-reauth-req 3
SM12DP2XA(config)# dot1x re-authentication
SM12DP2XA(config)# dot1x system-auth-control
SM12DP2XA(config)# dot1x timeout quiet-period 59000
```

enable

Modify enable password parameters.

Syntax

enable password [level <priv>] <password>

enable secret { 0 | 5 } [level <priv>] <password>

Parameter

password	Assign the privileged level clear password
secret	Assign the privileged level secret
<word32>	The UNENCRYPTED (cleartext) password
level	Set exec level password
<1-15>	Level number
0	Specifies an UNENCRYPTED password will follow
5	Specifies an ENCRYPTED secret will follow

EXAMPLE

```
SM12DP2XA(config)# enable password level 15 admin
SM12DP2XA(config)# enable password super-user
SM12DP2XA(config)# enable password level 15 superuser
SM12DP2XA(config)# enable secret 0 adv-Admin
SM12DP2XA(config)# enable secret 5 AdvAdmin
SM12DP2XA(config)#
```

event

Configure Trap event severity levels.

Syntax

event group { AC-Power | ACL | ACL-Log | Access-Mgmt | Auth-Failed | AUTO-SAVING | Cold-Start | Config-Info | DI-1-Normal | Digital-Out | Firmware-Upgrade | Import-Export | LACP | Link-Status | Login | Logout | Mgmt-IP-Change | Module-Change | NAS | Password-Change | PoE-PD-On | Port-Security | PWR-1-Off-On | PWR-2-Off-On | Spanning-Tree | Warm-Start | DC-Power | Battery-Power | BCS-Protection | DMS | Advanced | Dying-Gasp | PoE-Auto-Check | Poe-Auto-Power-Reset | FAN | ZTU-FAIL | Surveillance | SCP-Success | SCP-Fail } { level <lvl> | syslog { enable | disable } | trap { enable | disable } | smtp { enable | disable } | ipush { enable | disable } }

event group { PWR-1-On-Off | PWR-2-On-Off | DI-1-Abnormal | Loop-Protect | Temperature | Voltage | Rapid-Ring-Break | Rapid-Chain-Break | Rapid-Ring-Error | PoE-PD-Off | Over-Max-PoE-Power-Limitation | PoE-PD-Over-Current | OTP | MRP-Event } { level <lvl> | syslog { enable | disable } | trap { enable | disable } | smtp { enable | disable } | ipush { enable | disable } | digital-out { enable | disable } }

Parameters

Group	Configure trap event severity level			
<word32>	AC-Power	ACL	ACL-Log	Access-Mgmt
	Auth-Failed	BCS-Protection	Cold-Start	Config-Info
	DC-Power	DMS	Dying-Gasp	FAN
	Firmware-Upgrade	Import-Export	LACP	Link-Status
	Login	Logout	Loop-Protect	Mgmt-IP-Change
	Module-Change	NAS	Password-Change	Port-Security
	Rapid-Chain-Break	Rapid-Ring-Break	Rapid-Ring-Error	SCP-Fail
	SCP-Success	Spanning-Tree	Temperature	Voltage
	Warm-Start			
level	Severity level			
smtp	smtp mode			
syslog	syslog mode			
trap	trap mode			
<0-7>	<0> Emergency ,<1> Alert ,<2> Critical ,<3> Error ,<4> Warning ,<5> Notice ,<6> Informationl ,			
	<7> Debug			
disable	smtp mode disable			
enable	smtp mode enable			
disable	syslog mode disable			
enable	syslog mode enable			
disable	trap mode disable			

enable trap mode enable

EXAMPLE

```
SM12DP2XA(config)# event group dms level 1
SM12DP2XA(config)# event group acl trap enable
SM12DP2XA(config)# event group Dying-Gasp smtp enable
SM12DP2XA(config)# event group Voltage trap enable
SM12DP2XA(config)# event group Voltage syslog enable
SM12DP2XA(config)#
```

exec-timeout

Set exec-timeout autologout period.

Syntax

exec-timeout autologout { 0 | 1 | 2 | 3 | 4 | 5 | 10 | 20 | 30 | 40 | 50 | 60 }

Parameters

0	off (no timeout period)
1	1min
10	10min (default)
2	2min
20	20min
3	3min
30	30min
4	4min
40	40min
5	5min
50	50min
60	60min

EXAMPLE

```
SM12DP2XA(config)# exec-timeout autologout 60
SM12DP2XA(config)# exec-timeout autologout 0
SM12DP2XA(config)#
```

Auto-Logout Timeout: After you change the Auto-Logout timeout and then log out and log back in, the Auto-Logout timeout setting will be the setting saved to the start-up config file.

When the Auto-Logout timeout setting is changed, it writes directly to running-config.

To save the timeout change to start-up config, you must execute a save to startup-config.
To examine the running-config, you can run the CLI command “showing running-config” or in the Web UI just log out and log back in again.
To save the timeout change into startup-config, you must do a save to startup-config and then reboot the switch.
In summary:

- When you power on the switch, it will get the settings from startup-config.
- When you logout and login (without switch reboot), the switch will get the timeout settings from startup-config.
- When you reload defaults, the switch will get the timeout settings default-config.

For the “Save to start-up config” behavior, if you don’t save the config, when you change the timeout setting but logout, at the next login the timeout setting remains unchanged as the setting in start-up config.

If you save timeout setting to start-up config:	If you don’t save timeout setting to start-up config:
When you change the timeout setting and save to startup-config (click the disc icon), the changed timeout setting will be applied to running-config and start-up config immediately.	When the you change the timeout setting (without save to startup-config), the timeout change will be applied to running-config immediately.
After Logout and login, the timeout setting will be the setting saved in start-up config.	After Logout and login, the timeout setting will be the setting saved in start-up configure.
After a switch reboot, the timeout setting will be the setting saved in start-up config.	After you reboot the switch, the timeout setting will be the setting saved in start-up config.

exit

Exit from current mode.

Syntax

exit <cr>

Parameters

```
SM12DP2XA(config)# exit?
    exit    Exit from current mode
    <cr>
SM12DP2XA(config)# exit ?
    <cr>
SM12DP2XA(config)# exit
SM12DP2XA#
```

gvrp

Configure the GVRP feature. GVRP (GARP VLAN Registration Protocol) is used for dynamically registering VLANs on ports, as specified in IEEE 802.1Q-2005, clause 11.

Syntax

gvrp

gvrp max-vlans <1-4095>

gvrp time { [join-time <1-20>] [leave-time <60-300>] [leave-all-time <1000-5000>] }*1

Parameters

max-vlans	Number of simultaneous VLANs that GVRP can control
time	Configure GARP protocol timer parameters. IEEE 802.1D-2004, clause 12.11.
<cr>	

EXAMPLE

```
SM12DP2XA(config)# gvrp max-vlans 1000
SM12DP2XA(config)# gvrp time join-time 6 leave-all-time 2000 leave-time 100
SM12DP2XA(config)#
```

hostname

Set system's network name.

Syntax

hostname <hostname>

Parameter

<line128>	Set this system's network name.

EXAMPLE

```
SM12DP2XA(config)# hostname BobB sysNet1
BobB sysNet1 (config)# hostname sm12dp2xa
sm12dp2xa(config)# hostname SM12DP2XA
SM12DP2XA(config)#
```

interface

Select an interface to configure. See chapter Interface Config Mode Commands on page 157.

Syntax

interface (<port_type> [<plist>])

interface vlan <vlist>

Parameters

<port_type>	* or GigabitEthernet or 10GigabitEthernet
*	All switches or All ports
GigabitEthernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
vlan	VLAN interface configurations
<vlan_list>	List of VLAN interface numbers, 1-4095
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet

EXAMPLE 1: Show all interface config command parameters:

```
SM12DP2XA(config)# interface GigabitEthernet 1/1-13
SM12DP2XA(config-if)#
```

EXAMPLE 2: Show all interface config commands available:

```
SM12DP2XA(config-if)# <tab>
access-list                aggregation           broadcast-storm-protection  description
do                         dot1x                 duplex                      end
excessive-restart          exit                  flowcontrol                 frame-length-check
gvrp                       help                  ip                          ipv6
lacp                       lldp                  loop-protect                mac
mtu                        mvr                   no                          platform
port-security              priority-flowcontrol  pvlan                       qos
rmon                       sflow                 shutdown                    spanning-tree
speed                      switchport            udld
```

EXAMPLE 3: Show all interface VLAN config commands available:

```
SM12DP2XA(config)# interface vlan 333
SM12DP2XA(config-if-vlan)# ?
    do      To run exec commands in config mode
    end     Go back to EXEC mode
    exit    Exit from current mode
    help    Description of the interactive help system
```

```
    ip      Interface Internet Protocol config commands
    ipv6    IPv6 configuration commands
    no      Negate a command or set its defaults
SM12DP2XA(config-if-vlan)#
```

EXAMPLE 4: Configure switchport:

```
SM12DP2XA(config-if)# switchport <tab>
access     forbidden  hybrid     mode       trunk      vlan       voice
SM12DP2XA(config-if)# switchport mode ?
    access    Set mode to ACCESS unconditionally
    hybrid    Set mode to HYBRID unconditionally
    trunk     Set mode to TRUNK unconditionally
SM12DP2XA(config-if)# switchport access ?
    vlan    Set VLAN when interface is in access mode
SM12DP2XA(config-if)# switchport access vlan ?
    <vlan_id>    VLAN ID of the VLAN when this port is in access mode
SM12DP2XA(config-if)# switchport access vlan 10 ?
    <cr>
SM12DP2XA(config-if)#
```

EXAMPLE 5: Configure interface VLAN:

```
SM12DP2XA(config)# interface vlan ?
    <vlan_list>    List of VLAN interface numbers, 1~4095
SM12DP2XA(config)# interface vlan 10 ?
    <cr>
SM12DP2XA(config)# interface vlan 10
SM12DP2XA(config-if-vlan)# ?
    do      To run exec commands in config mode
    end     Go back to EXEC mode
    exit    Exit from current mode
    help    Description of the interactive help system
    ip      Interface Internet Protocol config commands
    ipv6    IPv6 configuration commands
    no      Negate a command or set its defaults
SM12DP2XA(config-if-vlan)#
```

EXAMPLE 6: Configure port security for an interface:

```
SM12DP2XA(config-if)# port-security max 500
SM12DP2XA(config-if)# port-security sticky 00-c0-f2-49-38-bb vlan 2
SM12DP2XA(config-if)# port-security violation trap-shutdown
SM12DP2XA(config-if)# end
SM12DP2XA# show port-security port
GigabitEthernet 1/1
-------------------
MAC Address       VID   State      Added                    Age/Hold Time
----------------  ----  ----------  -------------------------  -------------
<none>

GigabitEthernet 1/2
-------------------
MAC Address       VID   State      Added                    Age/Hold Time
----------------  ----  ----------  -------------------------  -------------
<none>

GigabitEthernet 1/3
-------------------
MAC Address       VID   State      Added                    Age/Hold Time
----------------  ----  ----------  -------------------------  -------------
<none>

GigabitEthernet 1/4
-------------------
MAC Address       VID   State      Added                    Age/Hold Time
----------------  ----  ----------  -------------------------  -------------
SM12DP2XA# show port-security switch
Users:
L = Limit Control
8 = 802.1X
V = Voice VLAN
Interface              Users  State         MAC Cnt
---------------------  -----  ------------  -------
GigabitEthernet 1/1     L--    Ready              0
```

```
GigabitEthernet 1/2      L--    Ready              0
GigabitEthernet 1/3      L--    Ready              0
GigabitEthernet 1/4      L--    Ready              0
GigabitEthernet 1/5      L--    Ready              0
GigabitEthernet 1/6      ---    No users           0
GigabitEthernet 1/7      ---    No users           0
GigabitEthernet 1/8      ---    No users           0
GigabitEthernet 1/9      ---    No users           0
GigabitEthernet 1/10     ---    No users           0
GigabitEthernet 1/11     ---    No users           0
GigabitEthernet 1/12     ---    No users           0
GigabitEthernet 1/13     ---    No users           0
GigabitEthernet 1/14     ---    No users           0
10GigabitEthernet 1/1    ---    No users           0
10GigabitEthernet 1/2    ---    No users           0
SM12DP2XA#
```

EXAMPLE 7: Negate port security for an interface:

```
SM12DP2XA(config-if)# no port-security ?
    maximum      Maximum number of MAC addresses that can be learned on this set of interfaces.
    sticky       Enable/disable port security sticky function per interface.
    violation    The action involved with exceeding the limit.
    <cr>
SM12DP2XA(config-if)# no port-security
SM12DP2XA(config-if)# no port-security sticky
SM12DP2XA(config-if)# no port-security maximum
SM12DP2XA(config-if)# no port-security violation
SM12DP2XA(config-if)#
```

ip

Configure Internet Protocol parameters.

Syntax

ip arp inspection

ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>

ip arp inspection translate [interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>]

ip arp inspection vlan <in_vlan_list>

ip arp inspection vlan <in_vlan_list> logging { deny | permit | all }

ip dhcp excluded-address <low_ip> [<high_ip>]

ip dhcp pool <pool_name>

ip dhcp relay

ip dhcp relay information option

ip dhcp relay information policy { drop | keep | replace }

ip dhcp server

ip dhcp server per-port {vlan}

ip dhcp snooping

ip dns proxy

ip domain name { <v_domain_name> | dhcp [ipv4 | ipv6] [interface vlan <v_vlan_id_dhcp>] }

ip gateway interface <ifc>

ip helper-address <v_ipv4_ucast>

ip http port <port>

ip http secure-certificate { upload <url_file> [pass-phrase <pass_phrase>] | generate }

ip http secure-server port <port>

ip igmp host-proxy [leave-proxy]

ip igmp snooping

ip igmp snooping vlan <v_vlan_list>

ip igmp ssm-range <v_ipv4_mcast> <ipv4_prefix_length>

ip igmp unknown-flooding

ip link-local interface <ifc>

ip name-server [<order>] { <v_ipv4_addr> | { <v_ipv6_addr> [interface vlan <v_vlan_id_static>] } | dhcp [ipv4 | ipv6]
[interface vlan <v_vlan_id_dhcp>]}

ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>

ip routing

ip scp server { enable | disable }

ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mac_var>

ip ssh

ip ssh keyregen

ip ssh port <port>

ip telnet port <port>

ip verify source

ip verify source translate

Parameters

arp	Address Resolution Protocol
dhcp	Dynamic Host Configuration Protocol
dns	Domain Name System
domain	IP DNS Resolver
gateway	Gateway address binding interface
helper-address	DHCP relay server
http	Hypertext Transfer Protocol
igmp	Internet Group Management Protocol
link-local	Link-Local address binding interface
name-server	Domain Name System
route	Add IP route
routing	Enable routing for IPv4 and IPv6
scp	Secure Copy Protocol function
source	source command
ssh	Secure Shell
telnet	TELNET
verify	verify command
inspection	ARP inspection
entry	arp inspection entry
interface	arp inspection entry interface config
<port_type>	Port type in Fast, Giga ethernet
<port_type_id>	Port ID in the format of switch-no/port-no
<vlan_id>	Select a VLAN id to configure
<mac_ucast>	Select a MAC address to configure
<ipv4_ucast>	Select an IP Address to configure
deny	log denied entries
permit	log permitted entries
all	log all entries
translate	arp inspection translate all entries

vlan arp inspection vlan setting
<vlan_list> arp inspection vlan list
relay DHCP relay agent information
information DHCP information option <Option 82>
option DHCP option
information DHCP information option(Option 82)
policy Policy for handling the receiving DHCP packet already include the information option
drop Drop the package when receive a DHCP message that already contains relay information
keep Keep the original relay information when receive a DHCP message that already contains it
replace Replace the original relay information when receive DHCP message that already contains it
server Enable DHCP server
snooping DHCP snooping
proxy DNS proxy service
secure-redirect Secure HTTP web rediction
secure-server Secure HTTP web server
snooping Snooping IGMP
<word16> Profile name in 16 char's
vlan IGMP VLAN
ssm-range IPv4 address range of Source Specific Multicast
<ipv4_mcast> Valid IPv4 multicast address
<4-32> Prefix length ranges from 4 to 32
unknown-flooding Flooding unregistered IPv4 multicast traffic
<ipv4_ucast> A valid IPv4 unicast address
dhcp Dynamic Host Configuration Protocol
interface Select an interface to configure
vlan VLAN Interface
<vlan_id> VLAN identifier(s): VID
<ipv4_addr> Network
<ipv4_netmask> Netmask
<ipv4_addr> Gateway
binding ip source binding
interface ip source binding entry interface config
<port_type> * or Gigibitethernet
* All switches or All ports
Gigabitethernet1 Gigabitethernet Port
<port_type_id> Port ID; format: switch-no/port-no; 1/1-14 for Gb Ethernet, 1/1-2 for 10Gb Ethernet

<vlan_id>	Select a VLAN id to configure
<ipv4_ucast>	Select an IP Address to configure
<ipv4_netmask>	Select a subnet mask to configure
<mac_ucast>	Select a MAC address to configure
source	verify source
limit	limit command
<0-2>	the number of limit
translate	ip verify source translate all entries
loggin	ARP inspection vlan loging mode config
<domain_name>	Default domain name
dhcp	Dynamic Host Configuration Protocol
interface	Select an interface to configure
ipv6	DNS setting is derived from DHCPv6; Default selection
<vlan_id>	VLAN identifier (VID)
ipv6	DNS setting is derived from DHCPv6; Default selection
<1-65534>	Port number
generate	Generate a new self-signed RSA certificate
upload	Upload a certificate PEM file
<url_file>	Uniform Resource Locator. A specific character string that constitutes a reference to a resource. Syntax: <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name> If the following special characters: space!"#$%&'()*+,/:;<=>?@[\]^`{|}~ need to be contained in the input url string, they should have percent-encoded. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score(_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.
<0-3>	Preference of DNS server. Default selection is 0
<ipv4_addr>	A valid IPv4 unicast address
<ipv6_addr>	A valid IPv6 unicast address
ipv6	DNS setting is derived from DHCPv6
server	support scp server
disable	Set mode to scp Disable
enable	Set mode to scp Enable
keyregen	Regenerate ssh key
port	Service port number
A.B.C.D	Lighting Server's IP address

EXAMPLE 1

```
SM12DP2XA(config)# ip arp inspection
SM12DP2XA(config)# ip dhcp relay
SM12DP2XA(config)# ip dns proxy
SM12DP2XA(config)# ip helper-address 192.168.1.77
SM12DP2XA(config)# ip routing
SM12DP2XA(config)# ip ssh
SM12DP2XA(config)# ip verify source translate
IP Source Guard:
       Translate 0 dynamic entries into static entries.
SM12DP2XA(config)# ip dhcp server per-port
SM12DP2XA(config)# ip domain name dhcp interface vlan 200 ipv6
SM12DP2XA(config)# ip gateway interface 200
SM12DP2XA(config)# ip http port 777
SM12DP2XA(config)# ip http secure-server port 888
SM12DP2XA(config)# ip http secure-certificate generate
SM12DP2XA(config)# ip link-local interface 1
SM12DP2XA(config)# ip name-server 0 197.166.1.100
SM12DP2XA(config)#
```

EXAMPLE 2

```
SM12DP2XA(config)# ip scp server enable
SM12DP2XA(config)# ip ssh port 999
SM12DP2XA(config)# ip ssh port 555
SM12DP2XA(config)# ip telnet port 333
<Disconnected>  >>>>>>>>>>
Username: admin
Password:
SM12DP2XA#
```

EXAMPLE 3

```
SM12DP2XA(config)# ip ssh keyregen
W ssh 01:49:53 132/ssh_change_key#503: Warning: It will take some time. Please wait for key
generating complete...

W ssh 01:50:04 132/ssh_change_key#538: Warning: ECDSA : Public key portion is:
 521 ecdsa-sha2-nistp521 AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBAH
dzCVJuGqawCAFsr7XBQPABAgvTsLRGKGkU1H7udELGWrj5ApJ4NB7fEjhDnDlK0FjiFSMoEggijuSm49
aIRJMRwEKOzF7IJCXxXwZXxUQP6h1HlcvLGPO9cpgx/0tlF3ylWW4u67IHoqG5WUmRfOc95rPIBAXK5E
gWyLrtu4CiZX0yg==
ECDSA: md5 5c:ef:09:91:95:64:8c:82:69:81:76:16:03:b6:aa:db


W ssh 01:50:04 132/ssh_change_key#555: Warning: Key generation completed

SM12DP2XA(config)#
```

EXAMPLE 4: Use DHCP option 229 to specify a lighting server available to the client. Enable this feature for any ports used for lighting nodes as it significantly reduces the delay time between lighting node connection to a port and when the switch allows network communication from the lighting node to the lighting gateway. Note: If multicast traffic is not allowed on your network, you can configure the network DHCP server to pass the lighting gateway server IP address in DHCP Option 229 (added at FW v7.20.0106). With the switch acting as a DHCP Server, it will insert operation 229 into DHCP offer packets and DHCP ACK packets. After receiving DHCP discover packets, it will insert option 229 for all DHCP clients as long as the DHCP Server is configured with Option 229. This option is configurable via the Web UI, SNMP, and CLI.

```
SISGM1040-284-LRT(config-dhcp-pool)# lighting server ?
A.B.C.D Server's IP address
SISGM1040-284-LRT(config-dhcp-pool)# lighting server 192.168.1.101
SISGM1040-284-LRT(config-dhcp-pool)#
```

Messeges:

VLAN ID 10 is not existed. Please create it and set its IP.

% Invalid word detected at '^' marker.

ipmc

IPv4/IPv6 multicast configuration. IPMC (IP MultiCast) supports IPv4 and IPv6 multicasting (IPMCv4 and IPMCv6).

Syntax

ipmc profile

ipmc profile <profile_name>

ipmc range <entry_name> { <v_ipv4_mcast> [<v_ipv4_mcast_1>] | <v_ipv6_mcast> [<v_ipv6_mcast_1>] }

Parameters

profile	IPMC profile configuration
range	A range of IPv4/IPv6 multicast addresses for the profile
< word16>	Range entry name in 16 characters
<ipv4_mcast>	Valid IPv4 multicast address
<ipv6_mcast>	Valid IPv6 multicast address
<ipv4_mcast>	Valid IPv4 multicast address that is not less than start address
default	Set a command to its defaults
description	Additional description about the profile in 64 characters
do	To run exec commands in config mode
end	Go back to EXEC mode
exit	Exit from current mode
help	Description of the interactive help system
no	Negate a command or set its defaults
deny	Deny matching addresses
permit	Permit matching addresses
log	Log when matching
next	Specify next entry used in profile. Default: Add entry last

EXAMPLE

```
SM12DP2XA(config)# ipmc range Range1 224.99.99.99
SM12DP2XA(config)# ipmc profile test
SM12DP2XA(config-ipmc-profile)# description IPMC filtering profile 2-11-21
SM12DP2XA(config)# ipmc range Range1 224.99.99.99
SM12DP2XA(config)# do show ipmc range
Range Name   : Range1
Start Address: 224.99.99.99
End Address  : 224.99.99.99
SM12DP2XA(config)#
```

Messages:

% Invalid next entry name Range2.

% Range1 is not a rule set in profile Profile1.

ipv6

IPv6 configuration commands.

Syntax

ipv6 mld host-proxy [leave-proxy]

ipv6 mld snooping

ipv6 mld snooping vlan <v_vlan_list>

ipv6 mld ssm-range <v_ipv6_mcast> <ipv6_prefix_length>

ipv6 mld unknown-flooding

ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }

Parameters

mld	Multicasat Listener Discovery
route	Configure static routes
host-proxy	MLD proxy configuration
snooping	Snooping MLD
ssm-range	IPv6 address range of Source Specific Multicast
unknown-flooding	Flooding unregistered IPv6 multicast traffic
leave-proxy	MLD proxy for leave configuration
vlan	MLD VLAN
<vlan_list>	VLAN identifier(s): VID
<ipv6_mcast>	Valid IPv6 multicast address
X:X:X:X::X/<0-128>	IPv6 prefix x:x::y/z
<ipv6_subnet>	IPv6 prefix x:x::y/z
<ipv6_ucast>	IPv6 unicast address (except link-local address) of next-hop
interface	Select an interface to configure

EXAMPLE

```
SM12DP2XA(config)# ipv6 mld host-proxy leave-proxy
SM12DP2XA(config)# ipv6 mld snooping vlan 1
SM12DP2XA(config)# ipv6 mld snooping vlan 200
SM12DP2XA(config)# ipv6 mld unknown-flooding
SM12DP2XA(config)#
```

lacp

Configure LACP (Link Aggregation Control Protocol) parameters. 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. An LACP trunk group with more than one ready member ports is a “real trunked” group. An LACP trunk group with only one or no ready member ports is not a “real trunked” group.

Syntax

lacp system-priority <v_1_to_65535>

lacp on-air index <v_1_to_8> { { port <port_type> <in_port_type_id> } | { couple-ip <ip1> <ip2> } }

Parameters

system-priority	System priority
<1-65535>	Priority value, lower means higher priority
on-air	On Air
system-priority	System priority
<1-65535>	Priority value, lower means higher priority
index	Index
<1-8>	1-8
couple-ip	Set couple ip address
port	Port
<ipv4_addr>	IPv4 Address

EXAMPLE

```
SM12DP2XA(config)# lacp system-priority 50
SM12DP2XA(config)# lacp on-air index 1 couple-ip 1.2.3.4 2.3.4.5
SM12DP2XA(config)#
```

Message: *LACP and Static aggregation can not both be enabled on the same ports*

line

Configure a terminal line.

Syntax

line { <0~16> | console 0 | vty <0~15> }

Parameters

<0~16>	List of line numbers
console	Console terminal line
0	Console Line number
vty	Virtual terminal
<0~15>	List of vty numbers
do	To run exec commands in config mode
editing	Enable command line editing
end	Go back to EXEC mode
exec-banner	Enable the display of the EXEC banner
exec-timeout	Set the EXEC timeout
exit	Exit from current mode
help	Description of the interactive help system
history	Control the command history function
length	Set number of lines on a screen
location	Enter terminal location description
motd-banner	Enable the display of the MOTD banner
no	Negate a command or set its defaults
privilege	Change privilege level for line
width	Set width of the display terminal
<0-1440>	Timeout in minutes
size	Set history buffer size
<0-32>	Number of history commands, 0 means disable
<0,3-512>	Number of lines on screen (0 for no pausing)
<line32>	One text line describing the terminal's location in 32 characters
level	Assign default privilege level for line
<0-15>	Default privilege level for line
<0,40-512>	Number of characters on a screen line (0 for unlimited width)

EXAMPLE

```
SM12DP2XA(config)# line 1
SM12DP2XA(config-line)# exec-banner
```

```
SM12DP2XA(config-line)# exec-timeout 1440
SM12DP2XA(config-line)# history size 14
SM12DP2XA(config-line)# exit
SM12DP2XA(config)#
```

lldp

Configure LLDP parameters. 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 MIB, making it possible for the information to be accessed by an NMS using a management protocol such as SNMP.

LLDP-MED (Media Endpoint Discovery) is an LLDP enhancement that provides auto-discovery of LAN policies, device location discovery, extended and automated power management of Power over Ethernet (PoE) end points, and inventory management, allowing network administrators to track their network devices.

Syntax

lldp holdtime <val>

lldp med datum { wgs84 | nad83-navd88 | nad83-mllw }

lldp med fast <v_1_to_10>

lldp med location-tlv altitude { meters | floors } <v_word11>

lldp med location-tlv civic-addr { { country <country> } | { state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | n ame | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code } <v_line> }

lldp med location-tlv elin-addr <v_word25>

lldp med location-tlv latitude { north | south } <v_word8>

lldp med location-tlv longitude { west | east } <v_word9>

lldp med media-vlan-policy <policy_index> { voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling } { untagged | tagged <v_vlan_id> [l2-priority <v_0_to_7>] } [dscp <v_0_to_63>]

lldp reinit <val>

lldp timer <val>

lldp transmission-delay <val>

Parameters

holdtime	Sets LLDP hold time (The neighbor switch will discarded the LLDP information after "hold time" multiplied with "timer" seconds).
med	Media Endpoint Discovery.
reinit	LLDP tx reinitialization delay in seconds.
timer	Sets LLDP TX interval (The time between each LLDP frame transmitted in seconds).
transmission-delay	Sets LLDP transmision-delay. LLDP transmission delay (the amount of time that the transmission of LLDP frames will delayed after LLDP configuration has changed) in seconds.)
<2-10>	2-10 seconds.
<1-10>	1-10 seconds.
<5-32768>	5-32768 seconds.
<1-8192>	1-8192 seconds.
datum	Datum (geodetic system) type.
fast	Number of times to repeat LLDP frame transmission at fast start.
location-tlv	LLDP-MED Location Type Length Value parameter.
media-vlan-policy	Use the media-vlan-policy to create a policy, which can be assigned to an interface.
nad83_mllw	Mean lower low water datum 1983
nad83_navd88	North American vertical datum 1983
wgs84	World Geodetic System 1984
altitude	Altitude parameter
meter	Altitude value
floors	Altitude value
civic-addr	Civic address information and postal information
country	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
state	National subdivisions (state, canton, region, province, prefecture).
county	County, parish, gun (Japan), district.
city	City, township, shi (Japan) - Example: Copenhagen.
district	City division, borough, city district, ward, chou (Japan).
block	Neighbourhood, block.
street	Street - Example: Poppelvej.
leading-street-direction	Leading street direction - Example: N.
trailing-street-suffix	Trailing street suffix - Example: SW.
street-suffix	Street suffix - Example: Ave, Platz.
house-no	House number - Example: 21.
house-no-suffix	House number suffix - Example: A, 1/2.
landmark	Landmark or vanity address - Example: Columbia University.

additional-info	Additional location info - Example: South Wing.
name	Name (residence and office occupant) - Example: Flemming Jahn.
zip-code	Postal/zip code - Example: 2791.
building	Building (structure) - Example: Low Library.
apartment	Unit (Apartment, suite) - Example: Apt 42.
floor	Floor - Example: 4.
room-number	Room number - Example: 450F.
place-type	Place type - Example: Office.
postal-community-name	Postal community name - Example: Leonia.
p-o-box	Post office box (P.O. BOX) - Example: 12345.
additional-code	Additional code - Example: 1320300003.
<string250>	Value for the corresponding selected civic address.
elin-addr	Emergency Location Identification # (e.g. E911, etc.), such as defined by TIA or NENA.
<dword25>	ELIN value
north	Setting latitude direction to north.
south	Setting latitude direction to south.
<word8>	Latitude degrees (0.0000-90.0000).
policy-list	Assignment of policies.
<range_list>	Policies to assign to the interface.
<0-31>	Policy id for the policy which is created.
voice	Create a voice policy.
voice-signaling	Create a voice signaling policy.
guest-voice-signaling	Create a guest voice signaling policy.
guest-voice	Create a guest voice policy.
softphone-voice	Create a softphone voice policy.
video-conferencing	Create a video conferencing policy.
streaming-video	Create a streaming video policy.
video-signaling	Create a video signaling policy.
tagged	The policy uses tagged frames.
<vlan_id>	The VLAN the policy uses tagged frames.
untagged	The policy uses un-tagged frames.
l2-priority	Layer 2 priority.
<0-7>	Priority 0-7
dscp	Differentiated Services Code Point.
<0-63>	DSCP value 0-63.

EXAMPLE

```
SM12DP2XA(config)# lldp holdtime 5
SM12DP2XA(config)# lldp med fast 5
SM12DP2XA(config)# lldp reinit 3
SM12DP2XA(config)# lldp transmission-delay 333
Note: According to IEEE 802.1AB-clause 10.5.4.2 the transmission-delay must not be larger than
LLDP timer * 0.25. LLDP timer changed to 1332
SM12DP2XA(config)# lldp med datum ?
    nad83-mllw      Mean lower low water datum 1983
    nad83-navd88    North American vertical datum 1983
    wgs84           World Geodetic System 1984
SM12DP2XA(config)# lldp med datum wgs84
SM12DP2XA(config)# lldp med location-tlv altitude ?
    floors    Specify the altitude in floor.
    meters    Specify the altitude in meters.
SM12DP2XA(config)# lldp med location-tlv altitude floors ?
    <word11>    Altitude value. Valid range -2097151.9 to 2097151.9
SM12DP2XA(config)# lldp med location-tlv altitude floors 34
SM12DP2XA(config)#
```

logging

Configure Syslog parameters.

Syntax

logging host { <ipv4_addr> | <domain_name> | <ipv6> }

logging on

logging port <port_no>

Parameters

host	Syslog host
<ipv4_ucast>	IP address of the log server
<hostname>	Donain name of the log server
on	Enable syslog server
<1-65535>	Port number
<domain_name>	The domain name provides a mechanism for naming resources on the Internet. A complete domain name consists of one or more subdomain names which are separated by dots(.)
<ipv4_ucast>	The IPv4 address of the log server.
<ipv6_ucast>	The IPv6 address of the log server.

EXAMPLE

```
SM12DP2XA(config)# logging host 192.168.1.30
SM12DP2XA(config)# logging on
SM12DP2XA(config)# logging port 514
SM12DP2XA(config)# logging host BobB
SM12DP2XA(config)#
```

loop-protect

Configure Loop protection parameters.

Syntax

loop-protect

loop-protect shutdown-time <0-604800>

loop-protect transmit-time <1-10>

Parameters

shutdown-time	Loop protection shutdown time interval
<0-604800>	Shutdown time in seconds
transmit-time	Loop protection transmit time interval
<1-10>	Transmit time in seconds

EXAMPLE

```
SM12DP2XA(config)# loop-protect
SM12DP2XA(config)# loop-protect shutdown-time 5000
SM12DP2XA(config)# loop-protect transmit-time 4
SM12DP2XA(config)#
```

mac

Configure MAC table entries.

Syntax

mac address-table aging-time <0,10-1000000>

mac address-table learning vlan <vlan_list>

mac address-table static <mac_addr> vlan <vlan_id> interface <port_type> <port_type_list>

Parameters

address-table	Mac Address Table
aging-time	Mac address aging time
<0,10-1000000>	Aging time in seconds, 0 disables aging
learning	Mac Learning
static	Static MAC address
<mac_addr>	48 bit MAC address: xx:xx:xx:xx:xx:xx
vlan	VLAN keyword
<vlan_id>	VLAN IDs 1-4095
interface	Select an interface to configure
<port_type>	Port type * or Gigabitethernet
*	All switches or All ports
Gigabitethernet	1 Gigabit Ethernet port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet

EXAMPLE

```
SM12DP2XA(config)# mac address-table aging-time 500000
SM12DP2XA(config)# mac address-table learning vlan 1
SM12DP2XA(config)# mac address-table static 00-c0-f2-49-38-bb vlan 1
Error: MAC address exists (system address)
Could not add mac address
SM12DP2XA(config)# mac address-table static 00-c0-f2-49-38-bb vlan 10
SM12DP2XA(config)#
```

map-api-key

Set Google Maps key string. You need a valid API key and a Google Cloud Platform billing account to access Google product. If no key is entered, DMS Map View will not be able to load Google Maps correctly.
See the Google website and follow the on-screen steps to get an API key:
https://developers.google.com/maps/documentation/directions/get-api-key

Syntax

map-api-key <key_str>

Parameters

map-api-key Set Google Maps key string.

EXAMPLE

```
SM12DP2XA(config)# map-api-key 8Axsntra&8>
SM12DP2XA(config)# do show map
Key   : 8Axsntra&8>
SM12DP2XA(config)#
```

monitor

Configure a MIRROR session.

Syntax

monitor session <session_number> [destination { interface (<port_type> [<di_list>]) | remote vlan <drvid> reflector-port <port_type> <rportid> } | source { interface (<port_type> [<si_list>]) [both | rx | tx] | remote vlan <srvid > | vlan <source_vlan_list> } | intermediate { interface (<port_type> [<ii_list>]) | remote vlan <irvid> }]

Parameters

<1>	MIRROR session number
destination	MIRROR destination interface or VLAN
intermediate	MIRROR intermediate interface, VLAN
source	MIRROR source interface, VLAN
interface	MIRROR destination interface
remote	MIRROR destination Remote
interface	MIRROR intermediate interface
remote	MIRROR intermediate Remote
interface	MIRROR source interface
remote	MIRROR source Remote
<vlan_list>	MIRROR source VLAN
vlan	MIRROR source VLAN
<port_type>	* or Gigabit Ethernet port
*	All switches or all ports.
<port_type_list>	Port list in 1/1-14 for Gigabitethernet. Port list in 1/1-2 for 10Gigabitethernet
GigabitEthernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
vlan	MIRROR intermediate Remote number
<vlan_id>	Remote MIRROR intermediate RMIRROR VLAN number
<port_type_list>	Port list for all port types
both	MIRROR source receive both
rx	MIRROR source receive Rx
tx	MIRROR source receive Tx

EXAMPLE

```
SM12DP2XA(config)# $tor session 1 destination interface GigabitEthernet 1/1
SM12DP2XA(config)# monitor session 1 source vlan 10,20
SM12DP2XA(config)# monitor session 1 destination interface * 1/3
```

```
SM12DP2XA(config)# monitor session 1 intermediate remote vlan 200
SM12DP2XA(config)# monitor session 1 source interface * rx
SM12DP2XA(config)# monitor session 1 source interface * tx
SM12DP2XA(config)#
```

Messages:

% Interface GigabitEthernet 1/2 already configured as destination port.

% No such interface type: d

mvr

Configure Multicast VLAN Registration. The MVR (Multicast VLAN Registration) protocol for Layer 2 (IP)-networks enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs. MVR is used to save bandwidth by preventing duplicate multicast streams being sent in the core network; instead the streams are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested them.

Syntax

mvr

mvr name <mvr_name> channel <profile_name>

mvr name <mvr_name> frame priority <cos_priority>

mvr name <mvr_name> frame tagged

mvr name <mvr_name> igmp-address <v_ipv4_ucast>

mvr name <mvr_name> last-member-query-interval <ipmc_lmqi>

mvr name <mvr_name> mode { dynamic | compatible }

mvr vlan <v_vlan_list> [name <mvr_name>]

mvr vlan <v_vlan_list> channel <profile_name>

mvr vlan <v_vlan_list> frame priority <cos_priority>

mvr vlan <v_vlan_list> frame tagged

mvr vlan <v_vlan_list> igmp-address <v_ipv4_ucast>

mvr vlan <v_vlan_list> last-member-query-interval <ipmc_lmqi>

mvr vlan <v_vlan_list> mode { dynamic | compatible }

Parameters

name	MVR multicast name
<word16>	MVR multicast VLAN name
channel	MVR channel configuration
<word16>	Profile name in 16 char's
frame	MVR control frame in TX
priority	Interface CoS priority
<0-7>	CoS priority ranges from 0 to 7
tagged	Tagged IGMP/MLD frames will be sent
igmp-address	MVR address configuration used in IGMP
<ipv4_ucast>	A valid IPv4 unicast address MVR multicast VLAN name
last-member-query-interval	Last Member Query Interval in tenths of seconds
<0-31744>	0 - 31744 tenths of seconds
mode	MVR mode of operation
dynamic	Dynamic MVR operation mode

compatible	Compatible MVR operation mode
vlan	MVR multicast vlan
<vlan_list>	MVR multicast VLAN list
channel	MVR channel configuration
<word16>	Profile name in 16 char's
frame	MVR control frame in TX
priority	Interface CoS priority
<0-7>	CoS priority ranges from 0 to 7
igmp-address	MVR address configuration used in IGMP
<ipv4_ucast>	A valid IPv4 unicast address
<vlan_list>	MVR multicast VLAN list
last-member-query-interval	Last Member Query Interval in tenths of seconds
<0-31744>	0 - 31744 tenths of seconds
compatible	Compatible MVR operation mode

EXAMPLE

```
SM12DP2XA(config)# mvr  vlan 10
SM12DP2XA(config)# mvr vlan 10 mode dynamic
SM12DP2XA(config)# mvr name mvr1 channel ch1
SM12DP2XA(config)#
```

Message: *W mvr 23:07:50 53/_mvr_vlan_warning_handler#4034:*

Warning: Please adjust the management VLAN ports overlapped with MVR source ports!

W lacp 23:07:50 33/rx_stev#766: Warning: An illegal loopback occurred on port 13

Meaning: The Management VLAN ports overlapped with MVR source ports.

Recovery: Adjust the MVR source ports so they do not overlap with the Management VLAN ports.

Messages:

% Invalid MVR VLAN ID 200.

% Invalid operation.

% Failed to set MVR interface channel.

Percepxion

Description: Percepxion configuration; enter Percepxion Config mode and set Percepxion parameters.

Percepxion is a cloud or on-premise portal for the centralized management of multiple Lantronix switches. A browser-based interface allows an administrator to view status, send commands, view logs and charts, and update firmware. Each Lantronix device can communicate with the cloud server or on-premise server, sending status updates and responding to commands sent by the server.

The switch requires a unique Device ID to communicate with the Percepxion portal. The ID is viewable in the Percepxion settings by running the 'show' command at the 'config-percepxion' command mode. If a device is not already pre-configured with the ID, the ID must be provisioned using Lantronix Provisioning Manager (LPM).

The Percepxion client follows a sequence of steps to connect to the Percepxion server, send status updates, check for firmware and configuration updates, and respond to commands from the server. This series of steps is the same each time the client starts - at boot, or if the client is enabled. Any changes to the Percepxion Device ID, or registration settings require the Percepxion client to be disabled and re-enabled for the changes to take effect.

Percepxion client registration

The client will attempt to register to the Host using the project tag and device ID. If registration fails, the client will wait and retry. The client will retry until it is successful, or the client is disabled. Registration may fail if the Project Tag is invalid, the Device ID is invalid, the Host name cannot be resolved, or the Host is not reachable. Once registration is successful, the **Client State** will display **Registered** with the date and time of registration.

Telemetry

After registration, the client will connect to the Telemetry Host (the hostname is the same as the registration host provided during registration) and perform a telemetry handshake. This handshake may request that the client publish a set of statistics at regular intervals.

Messaging and Status Updates

After the telemetry handshake, the Percepxion client will connect to the messaging host to receive messages and publish status updates. If the connection fails, the client will wait and retry. The connection may fail if the messaging host name cannot be resolved, or the messaging host is not reachable. The client publishes status update messages (changes to the device attributes) at the interval defined by **Status Update Interval**. Each time a status update is published, the **Last status update** will be updated to indicate the elapsed time since the status was sent. The client also accepts command messages from the Percepxion server to perform actions, such as reboot.

Firmware updates and Configuration updates

The Percepxion client checks for firmware and configuration updates at the interval defined by the **Content Check Interval**. When the client checks for firmware or configuration updates, the **Last content check** will

be updated to indicate the elapsed time since the check was made. The **Available Firmware updates** and **Available Configuration updates** will indicate if an update was found on the server, or show *Not available*, if no updates were found.

Subcommands:

```
SISGM1040-284-LRT(config-percepxion)# ?
    active        Sets active connection to Connection <number>
    apply         Sets the mode on firmware updates
    connection    Sets the connection 1 or connection 2
    content       Sets the firmware and configuration check interval
    device        Sets the device attributes
    do            To run exec commands in config mode
    end           Go back to EXEC mode
    exit          Exit from current mode
    help          Description of the interactive help system
    no            Removes
    show          Displays the current configuration
    state         Percepxion state
    status        Sets the status update interval
```

Syntax and Parameters:

```
active connection connection <1|2>
```

- connection - sets the active connection

```
apply configuration updates <enable|disable>
```

- configuration updates - enables or disables configuration updates

```
apply firmware updates <enable|disable>
```

- firmware updates - enables or disables firmware updates

```
connection <1|2> connect to <cloud|on premise>
connection <1|2> host <host name>
connection <1|2> port <number>
connection <1|2> secure port <enable|disable>
connection <1|2> validate certificates <enable|disable>
```

- Sets the connection 1 or 2 settings.

- <1|2> - Indicates which connection to configure.
- connect to - sets the connect mode to cloud or on-premise
- host - sets the host name or IP address of the Percepxion server
- port - sets the port number of the Percepxion server. Default is 443.
- secure port - enables or disables secure port.
- validate certificates - If enabled use a certificate authority to validate the HTTPS certificate. Disabled by default.

```
content check interval <1-56160>
```

- check interval - sets the interval of time in minutes that the agent waits between checks for firmware or configuration updates. Valid values are 1 to 56160 minutes.

```
device description <device_desp>
device id <device_id>
device key <device_key>
device name <device_name>
```

- Sets the device attributes.
- device_desp - sets the description
- device_id – sets the device id
- device_key – sets the device key. After it is set, the key is displayed as <Configured>.
- device_name – sets the device name as it will be shown in Percepxion UI.

```
do <command>
```

- Run exec commands in the configuration mode

```
end
```

- Go back to exec mode

```
exit
```

- Exit from the current mode

```
help
```

- Shows description of the interactive help system

```
no device description
no device id
no device key
no device name
```

- Removes the value of a configuration setting

- description – removes the description
- id – removes the device id
- key – removes the device key
- name – removes the device name

```
show connection <1|2>
```

- Displays the current configuration of the specified connection

```
show statistics
```

- Displays the Percepxion statistics

```
state <disable|enable>
```

- Sets the Percepxion client state. Enabled by default.

```
status update interval <1-1440>
```

- update interval <1-1440> Sets the interval of time in minutes that the agent waits between sending its status to the Percepxion server. Valid values are 1 to 1440 minutes.

EXAMPLE

```
SM12DP2XA(config-percepxion)# active connection connection 1
SM12DP2XA(config-percepxion)# apply configuration updates enable
SM12DP2XA(config-percepxion)# apply firmware updates enable
SM12DP2XA(config-percepxion)# state enable
SM12DP2XA(config-percepxion)# connection 1 connect to cloud
SM12DP2XA(config-percepxion)# connection 1 connect to on premise
SM12DP2XA(config-percepxion)# connection 1 host 1.2.3.4
SM12DP2XA(config-percepxion)# connection 1 port 654
SM12DP2XA(config-percepxion)# connection 1 secure port enable
SM12DP2XA(config-percepxion)# connection 1 validate certificates enable
SM12DP2XA(config-percepxion)# content check interval 9000
SM12DP2XA(config-percepxion)# device description sm12xpa-sqa
SM12DP2XA(config-percepxion)# device id sn2846
SM12DP2XA(config-percepxion)# device key **************
SM12DP2XA(config-percepxion)# device name fortest
SM12DP2XA(config-percepxion)# do show version brief
Version      : SM12DP2XA (standalone) v7.20.0208
Build Date   : 2024-09-14T17:56:47+08:00
SM12DP2XA(config-percepxion)# no device key
SM12DP2XA(config-percepxion)# show connection 1
```

```
Percepxion Connection 1 Configuration:
Connect To : On Premise
Host : 1.2.3.4
Port : 654
Secure Port : Enabled
Validate Certificates: Enabled
SM12DP2XA(config-percepxion)# show statistics
Client Status : Running
Not registered -
Last Status Update : Not available
Last Content Check : Not available
Available Firmware Updates: Not available
Available Configuration Updates: Not available
SM12DP2XA(config-percepxion)# state enable
SM12DP2XA(config-percepxion)# status update interval 450
SM12DP2XA(config-percepxion)# end
SM12DP2XA(config-percepxion)# exit
SM12DP2XA(config)#
```

ntp

Configure NTP (Network Time Protocol) for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer. NTP is used to sync with the network time based Greenwich Mean Time (GMT).

Syntax

ntp <cr>

ntp automatic

ntp interval <interval>

ntp server <index_var> ip-address { <ipv4_var> | <ipv6_var> | <name_var> }

Parameters

automatic	Configure Automatic
interval	Configure NTP Time-Sync Interval
server	Configure NTP server
<1-5>	index number
ip-address	ip address
<ipv4_ucast>	ipv4 address
<ipv6_ucast>	ipv6 address
<domain_name>	domain name

EXAMPLE

```
SM12DP2XA(config)# ntp
SM12DP2XA(config)# ntp server 2 ip-address 192.168.1.30
SM12DP2XA(config)# ntp automatic
SM12DP2XA(config)# ntp interval 10
SM12DP2XA(config)# ntp server 1 ip-address BobB
SM12DP2XA(config)#
```

port-security

Enable/disable port security globally. You can use the Port Security commands to restrict input to an interface by limiting and identifying MAC addresses. Note that you can also configure port security for an interface.

Syntax

port-security

port-security aging

port-security aging time <v_10_to_10000000>

Parameters

aging	Enable/disable port security aging.
time	Time in seconds between check for activity on learned MAC addresses.
<10-10000000>	seconds

EXAMPLE

```
SM12DP2XA(config)# port-security aging time 50000
SM12DP2XA(config)# port-security aging
SM12DP2XA(config)# port-security
SM12DP2XA(config)#
```

privilege

Configure command privilege level parameters.

Syntax

privilege <mode_name> level <privilege> <cmd>

Parameters

config-vlan	VLAN Configuration Mode
configure	Global configuration mode
dhcp-pool	DHCP Pool Configuration Mode
exec	Exec mode
if-vlan	VLAN Interface Mode
interface	Port List Interface Mode
ipmc-profile	IPMC Profile Mode
line	Line configuration mode
rfc2544-profile	RFC2544 Profile Mode
snmps-host	SNMP Server Host Mode
stp-aggr	STP Aggregation Mode
level	Set privilege level of command
<0-15>	Privilege level
<line128>	Initial valid words and literals of the command to modify, in 128 characters

EXAMPLE

```
SM12DP2XA(config)# privilege <tab>
config-vlan   configure     dhcp-pool     exec          if-vlan
interface     ipmc-profile  line          snmps-host    stp-aggr
SM12DP2XA(config)# privilege dhcp-pool level 14 LINE
SM12DP2XA(config)# privilege ipmc-profile level 13 LINE
SM12DP2XA(config)#
```

radius-server

Configure RADIUS server parameters. Up to 5 servers are supported.

Syntax

radius-server attribute 32 <id>

radius-server attribute 4 <ipv4>

radius-server attribute 95 <ipv6>

radius-server deadtime <minutes>

radius-server host <host_name> [auth-port <auth_port>] [acct-port <acct_port>] [timeout <seconds>] [retransmit <retries>] [key { [unencrypted] <unencrypted_key> | encrypted <encrypted_key> }]

radius-server key { [unencrypted] <unencrypted_key> | encrypted <encrypted_key> }

radius-server retransmit <retries>

radius-server timeout <seconds>

Parameters

attribute	NAS attributes
deadtime	Time to stop using a RADIUS server that doesn't respond
host	Specify a RADIUS server
key	Set RADIUS encryption key
retransmit	Specify the number of retries to active server
timeout	Time to wait for a RADIUS server to reply
32	attribute number 32 = NAS-Identifier
4	attribute number 4 = NAS-IP-Address
95	attribute number 95 = NAS-IPv6-Address
<Minutes : 1-1440>	Time in minutes
<Host4 : ipv4_ucast>	IPv4 address
<Host6 : ipv6_ucast>	IPv6 address
<HostName : word1-255>	Hostname
<word1-255>	Hostname or IP address
acct-port	UDP port for RADIUS accounting server (e.g., port 1812 or 1645)
auth-port	UDP port for RADIUS authentication server (e.g., port 1813 or 1646)
key	Server specific key (overrides default)
retransmit	Specify the number of retries to active server (overrides default)
timeout	Time to wait for this RADIUS server to reply (overrides default)

<word1-63>	The UNENCRYPTED (Plain Text) secret key. Notice that you have no chance to get the Plain Text secret key after this command. The system will always display the ENCRYPTED password.
encrypted	Specifies an ENCRYPTED secret key will follow
unencrypted	Specifies an ENCRYPTED secret key will follow
<1-1000>	Number of retries for a transaction
<1-1000>	Wait time in seconds

EXAMPLE

```
SM12DP2XA(config)# radius-server attribute 32 a
SM12DP2XA(config)# radius-server host device key 12
SM12DP2XA(config)# radius-server host 1.2.3.4
SM12DP2XA(config)# radius-server host BobB key admin acct-port 1812 auth-port 1813
SM12DP2XA(config)# radius-server host BobB key admin acct-port 1645 auth-port 1646
SM12DP2XA(config)#
```

rapid-ring

Set Rapid Ring parameters. Other Ring technologies (e.g., Spanning Tree) must be disabled.

Syntax

rapid-ring entry <entryindex> role disabled

rapid-ring entry <entryindex> role master

rapid-ring entry <entryindex> role member

Parameters

entry	Set entry index
<uint8>	index
role	Set role value
disabled	role value disabled
master	role value master
member	role value member

EXAMPLE

```
SM12DP2XA(config)# rapid-ring entry 1 role master
SM12DP2XA(config)# rapid-ring entry 2 role member
SM12DP2XA(config)# rapid-ring entry 3 role member
SM12DP2XA(config)# rapid-ring entry 4 role member
SM12DP2XA(config)# do show rapid
Entry Index              : 1
Rapid Ring Role          : Master
Rapid Ring Port 1        : 1
Rapid Ring Port 2        : 2
Rapid Ring Port 1 State   : Discarding
Rapid Ring Port 2 State   : Discarding

Entry Index              : 2
Rapid Ring Role          : Member
Rapid Ring Port 1        : 3
Rapid Ring Port 2        : 4
Rapid Ring Port 1 State   : Discarding
Rapid Ring Port 2 State   : Discarding

Entry Index              : 3
Rapid Ring Role          : Member
```

```
Rapid Ring Port 1        : 5
Rapid Ring Port 2        : 6
Rapid Ring Port 1 State   : Discarding
Rapid Ring Port 2 State   : Discarding

Entry Index             : 4
Rapid Ring Role          : Member
Rapid Ring Port 1        : 7
Rapid Ring Port 2        : 8
Rapid Ring Port 2        : 8
Rapid Ring Port 2 State   : Discarding

Entry Index             : 5
Rapid Ring Role          : Disabled
Rapid Ring Port 1        : 9
Rapid Ring Port 2        : 10
Rapid Ring Port 1 State   : Forwarding
Rapid Ring Port 2 State   : Forwarding

Entry Index             : 6
Rapid Ring Role          : Disabled
Rapid Ring Port 1        : 11
Rapid Ring Port 2        : 12
Rapid Ring Port 1 State   : Forwarding
Rapid Ring Port 2 State   : Forwarding

Entry Index             : 7
Rapid Ring Role          : Disabled
Rapid Ring Port 1        : 15
Rapid Ring Port 2        : 16
Rapid Ring Port 1 State   : Forwarding
Rapid Ring Port 2 State   : Forwarding
SM12DP2XA(config)#
```

Messages: *R_RING_ICLI_system_set error in port 1, STP is enable*

rmon

Configure Remote Monitoring alarms and events.

Syntax

rmon alarm <id> { ifInOctets | ifInUcastPkts | ifInNUcastPkts | ifInDiscards | ifInErrors | ifInUnknownProtos | ifOutOctets | ifOutUcastPkts | ifOutNUcastPkts | ifOutDiscards | ifOutErrors } <ifIndex> <interval> { absolute | delta } rising-threshold <rising_threshold> [<rising_event_id>] falling-threshold <falling_threshold> [<falling_event_id>] { [rising | falling | both] }

rmon event <id> [log] [trap <community>] { [description <description>] }

Parameters

alarm	Configure an RMON alarm
event	Configure an RMON event
<1-65535>	Alarm entry ID
<WORD>	MIB object to monitor
<1-2147483647>	Sample interval
absolute	Test each sample directly
delta	Test delta between samples
rising-threshold	Configure the rising threshold
<-2147483648-2147483647>	rising threshold value
<0-65535>	Event to fire on rising threshold crossing
falling-threshold	Configure the falling threshold
<-2147483648-2147483647>	falling threshold value
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
both	Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default)
ifInOctets	The total number of octets received on the interface, including framing characters
ifInUcastPkts	The number of uni-cast packets delivered to a higher-layer protocol
ifInNUcastPkts	The number of broad-cast and multi-cast packets delivered to a higher-layer protocol
ifInDiscards	The number of inbound packets that are discarded even the packets are normal
ifInErrors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol
ifInUnknownProtos	Number of the inbound packets discarded for unknown or un-support protocol
ifOutOctets	The number of octets transmitted out of the interface , including framing characters
ifOutUcastPkts	The number of uni-cast packets that request to transmit
ifOutNUcastPkts	The number of broad-cast and multi-cast packets that request to transmit

ifOutDiscards	The number of outbound packets that are discarded event the packets is normal
ifOutErrors	The # of outbound packets that could not be transmitted because of errors
<uint>	ifIndex
<1-2147483647>	Sample interval
absolute	Test each sample directly
delta	Test delta between samples
rising-threshold	Configure the rising threshold
description	Specify a description of the event
log	Generate RMON log when the event fires
trap	Generate SNMP trap when the event fires

EXAMPLE

```
SM12DP2XA(config)# $9 absolute rising-threshold 0 falling-threshold 0 both
SM12DP2XA(config)# rmon alarm 1 ifOutErrors 1 50000 absolute rising-threshold 90000 999 falling-threshold -8888 both
SM12DP2XA(config)# rmon event 1 log trap cxvlk
SM12DP2XA(config)
```

Messages:

% Invalid: rising threshold must be larger than falling threshold

sflow

Configure Statistics flow. sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector. More information can be found at http://sflow.org.

Syntax

sflow agent-ip { ipv4 <v_ipv4_addr> | ipv6 <v_ipv6_addr> }

sflow collector-address [receiver <rcvr_idx_list>] [<ipv4_var> | <ipv6_var> | <domain_name>]

sflow collector-port [receiver <rcvr_idx_list>] <collector_port>

sflow max-datagram-size [receiver <rcvr_idx_list>] <datagram_size>

sflow timeout [receiver <rcvr_idx_list>] <timeout>

Parameters

agent-ip	The agent IP address used in UDP datagrams. Defaults to IPv4 loopback address.
Ipv4	ipv4 address
Ipv6	ipv6 address
<ipv4_addr>	ipv6 address
<ipv6_addr>	ipv4 address
collector-address	Collector address
collector-port	Collector UDP port
<1-65535>	Port Number
max-datagram-size	Maximum datagram size
<200-1468>	Bytes
timeout	Receiver timeout measured in seconds. The switch decrements the timeout once per second; and as long as it is non-zero, the receiver receives samples. Once the timeout reaches 0, the receiver and all its configuration is reset to defaults.
<0-2147483647>	Number in seconds

EXAMPLE

```
SM12DP2XA(config)# sflow agent-ip ipv4  192.168.1.30
SM12DP2XA(config)# sflow collector-port 3
SM12DP2XA(config)# sflow max-datagram-size 333
SM12DP2XA(config)# sflow timeout 3333
SM12DP2XA(config)#
```

smtp

Configure email parameters. Simple Mail Transfer Protocol is the message-exchange standard for the Internet. Configure the Switch as an SMTP client; the server is a remote device that will receive messages from the switch that alarm events occurred.

Syntax

smtp delete { server | username | sender | returnpath | mailaddress <index> }

smtp mailaddress <index> <mail_addr_name>

smtp returnpath <return_path>

smtp sender <sender_name>

smtp server <hostname>

smtp username <username> <password>

Parameters

delete	Delete command
mailaddress	Configure email address
returnpath	Configure email returnpath
sender	Configure email sender
server	Configure email server
username	Configure email user name

EXAMPLE

```
SM12DP2XA(config)# smtp mailaddress 1 jeffs@transition.com
SM12DP2XA(config)# smtp returnpath jeffsherm
SM12DP2XA(config)# smtp server server
SM12DP2XA(config)# smtp username 91ngine91ss 12345
SM12DP2XA(config)# smtp delete mailaddress 1
SM12DP2XA(config)#
```

snmp-server

Set SNMP server parameters.

Syntax

snmp-server

snmp-server access <group_name> model { v1 | v2c | v3 | any } level { auth | noauth | priv } [read <view_name>] [write <write_name>]

snmp-server community v2c <comm> [ro | rw]

snmp-server community v3 <v3_comm> [<v_ipv4_addr> <v_ipv4_netmask>]

snmp-server community writecommunity { enable | disable }

snmp-server contact <v_line255>

snmp-server engine-id local <engineID>

snmp-server host <conf_name>

snmp-server location <v_line255>

snmp-server security-to-group model { v1 | v2c | v3 } name <security_name> group <group_name>

snmp-server trap

snmp-server user <username> engine-id <engineID> [{ md5 { <md5_passwd> | { encrypted <md5_passwd_encrypt> } } | sha { <sha_passwd> | { encrypted <sha_passwd_encrypt> } } } [priv { des | aes } { <priv_passwd> | { encrypted <priv_passwd_encrypt> } }]]

snmp-server version { v1 | v2c | v3 }

snmp-server view <view_name> <oid_subtree> { include | exclude }

Parameters

access	access configuration
community	Set the SNMP community
contact	Set the SNMP server's contact string
engine-id	Set SNMP engine ID
host	Set SNMP host's configurations
location	Set the SNMP server's location string
security-to-group	security-to-group configuration
trap	Set trap's configurations
user	Set the SNMPv3 user's configurations
version	Set the SNMP server's version
view	MIB view configuration
<word32>	group name
model	security model
any	any security model

v1	v1 security model
v2c	v2c security model
v3	v3 security model
level	security level
auth	authNoPriv Security Level
noauth	noAuthNoPriv Security Level
priv	authPriv Security Level
read	specify a read view for the group
write	specify a write view for the group
<word32>	write view name
<word32>	read view name
writecommunity	SNMP server WriteCommunity
writecommunity	SNMP server WriteCommunity
<word32>	Community word
<ipv4_addr>	IPv4 address
<ipv4_netmask>	IPv4 netmask
<line255>	contact string
local	Set SNMP local engine ID
<word10-64>	local engine ID
<word10-64>	local engine ID
disable	Disable Trap mode
tcp	Use TCP for Trap mode
udp	Use UDP for Trap mode
v1	SNMP trap version 1
v2	SNMP trap version 2
v3	SNMP trap version 3
<word32>	93ngine93s name
engineID	Configure trap server’s engine ID
probe	Probe trap server’s engine ID
<word10-64>	trap server’s engine ID
<word32>	93ngine93s name
<domain_name>	hostname of SNMP trap host
<ipv4_ucast>	IP address of SNMP trap host
<ipv6_ucast>	IP address of SNMP trap host
retries	retires inform messages
<0-255>	retires times

timeout	timeout parmater
<0-2147>	timeout interval
<line255>	location string
do	To run exec commands in config mode
end	Go back to EXEC mode
exit	Exit from current mode
help	Description of the interactive help system
host	host configuration
informs	Send Inform messages to this host
no	Negate a command or set its defaults
shutdown	Disable the trap configuration
trapmode	Configure trap mode
version	Set SNMP trap version

EXAMPLE

```
SM12DP2XA(config)# snmp access Cdcc model any level auth write adminW read adminR
SM12DP2XA(config)# snmp community v3 Wcomm 1.2.3.4 255.255.255.0
SM12DP2XA(config)# snmp contact EngDesk tomt#trnst.com
SM12DP2XA(config)# snmp host ShostOne
SM12DP2XA(config)# snmp location Engineering-North
SM12DP2XA(config-snmps-host)#
SM12DP2XA(config-snmps-host)# informs retries 50 timeout 125
SM12DP2XA(config-snmps-host)# version v3 probe seucrityname
SM12DP2XA(config-snmps-host)# trapmode udp
SM12DP2XA(config-snmps-host)# informs retries 50 timeout 300
SM12DP2XA(config-snmps-host)# end
SM12DP2XA# con ter
SM12DP2XA(config)# snmp-server trap
SM12DP2XA(config)#
```

Messages:

The group name 'Cdcc' is not exist

The format of 'Engine ID' may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

system

Set system parameters.

Syntax

system contact <v_line128>

system description <sys_desc>

system location <v_line128>

system name <v_line128>

system reboot mode { enable | disable }

system reboot { [Sun <hour_v00_0_to_23> <min_v00_0_to_55>] [Mon <hour_v10_0_to_23> <min_v10_0_to_55>] [Tue <hour_v20_0_to_23> <min_v20_0_to_55>] [Wed <hour_v30_0_to_23> <min_v30_0_to_55>] [Thr <hour_v40_0_to_23> <min_v40_0_to_55>] [Fri <hour_v50_0_to_23> <min_v50_0_to_55>] [Sat <hour_v60_0_to_23> <min_v60_0_to_55>] }

Parameters

contact	Set the system contact string
description	Configure System Description
location	Set the system location string
name	Set the system model name string
reboot	Set the Switch Reboot mode and schedule
Fri	Configure Switch Reboot scheduling on Friday
Mon	Configure Switch Reboot scheduling on Monday
Sat	Configure Switch Reboot scheduling on Saturday
Sun	Configure Switch Reboot scheduling on Sunday
Thr	Configure Switch Reboot scheduling on Thursday
Tue	Configure Switch Reboot scheduling on Tuesday
Wed	Configure Switch Reboot scheduling on Wednesday
mode	Switch reboot mode
disable	Disable Switch Reboot
enable	Enable Switch Reboot

EXAMPLE

```
SM12DP2XA(config)# system contact jeffs
SM12DP2XA(config)# system description sm12dp2xa
SM12DP2XA(config)# system location mtka engineering
SM12DP2XA(config)# system name sm12dp2xa 4 docs
sm12dp2xa 4 docs(config)# system name SM12DP2XA
SM12DP2XA(config)#
```

tacacs-server

Configure TACACS+. TACACS+ provides separate authentication, authorization and accounting services. Up to 5 servers are supported.

Syntax

tacacs-server deadtime <minutes>

tacacs-server host <host_name> [port <port>] [timeout <seconds>] [key { [unencrypted] <unencrypted_key> | encrypted <encrypted_key> }]

tacacs-server key { [unencrypted] <unencrypted_key> | encrypted <encrypted_key> }

tacacs-server timeout <seconds>

Parameters

deadtime	Time to stop using a TACACS+ server that doesn't respond
host	Specify a TACACS+ server
key	Set TACACS+ encryption key
timeout	Time to wait for a TACACS+ server to reply (overrides default)
1-1440>	Time in minutes
<word1-255>	Hostname or IP address
<ipv4_ucast>	IPv4 address
<ipv6_ucast>	IPv6 address
port	TCP port for TACACS+ server
<0-65535>	TCP port number
key	Server specific key (overrides default)
<word1-63>	The UNENCRYPTED (Plain Text) secret key. Notice that you have no chance to get the Plain Text secret key after this command. The system will always display the ENCRYPTED password.
encrypted	Specifies an ENCRYPTED secret key will follow
unencrypted	Specifies an UNENCRYPTED secret key will follow
port	TCP port for TACACS+ server
timeout	Time to wait for this TACACS+ server to reply (overrides default)
<0-65535>	TCP port number
<1-1000>	Wait time in seconds
<word4-224>	The ENCRYPTED (hidden) secret key. Notice the ENCRYPTED secret key will be decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally.

EXAMPLE

```
SM12DP2XA(config)# tacacs-server deadtime 300
SM12DP2XA(config)# tacacs-server host 192.168.1.2
SM12DP2XA(config)# tacacs-server key 33
SM12DP2XA(config)# tacacs-server timeout 300
SM12DP2XA(config)# tacacs-server host 1.2.3.4 key admin01 port 555 timeout 300
SM12DP2XA(config)# tacacs-server key encrypted admin1admin2admin3!@#
SM12DP2XA(config)# tacacs-server key unencrypted admin
SM12DP2XA(config)#
```

tzidx

Configure timezone city/area.

Syntax

tzidx <idx_var>

Parameters

<int> index of city/area

EXAMPLE

```
SM12DP2XA(config)# tzidx?
    tzidx    Configure timezone city/area
SM12DP2XA(config)# tzidx 1
SM12DP2XA(config)# clock timezone test  8
SM12DP2XA(config)# tzidx 0
SM12DP2XA(config)# tzidx 1
SM12DP2XA(config)# tzidx 2
SM12DP2XA(config)#
```

udld

Enable UDLD in aggressive or normal mode and set the configurable message timer on all fiber-optic ports. Uni Directional Link Detection monitors the configuration of links between UDLD devices and ports.

Syntax

udld { aggressive | enable | message time-interval <v_interval> }

Parameters

aggressive	Enables UDLD in aggressive mode on all fiber-optic ports.
enable	Enables UDLD in normal mode on all fiber-optic ports.
message	time-interval
time-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 7-90 seconds (currently default message time interval 7 seconds is supported).

EXAMPLE

```
SM12DP2XA(config)# udld aggressive
SM12DP2XA(config)# udld enable
SM12DP2XA(config)# udld message time-interval 7
SM12DP2XA(config)#
```

upnp

Configure UpnP (Universal Plug and Play) parameters.

Syntax

upnp

upnp advertising-duration <66-86400>

upnp ttl <1-255>

Parameters

advertising-duration	Set advertising duration
ttl	Set TTL value
<100-86400>	advertising duration
<1-255>	TTL value

EXAMPLE

```
SM12DP2XA(config)# upnp advertising-duration 5000
SM12DP2XA(config)# upnp ttl 50
SM12DP2XA(config)#
```

username

Establish User Name Authentication.

Syntax

username <username> privilege <priv> password encrypted <encry_password>

username <username> privilege <priv> password none

username <username> privilege <priv> password unencrypted <password>

Parameters

<Username >	User name allows letters, numbers and underscores
privilege	Set user privilege level
< 0-15>	User privilege level
password	Specify the password for the user
encrypted	Specifies an ENCRYPTED password will follow
none	NULL password
unencrypted	Specifies an UNENCRYPTED password will follow
< line31>	The UNENCRYPTED (Plain Text) user password. Any printable characters including space is accepted.Notice that you have no change to get the Plain Text password after this command. The system will always display the ENCRYPTED password.
< word4-44>	The ENCRYPTED (hidden) user password. Notice the ENCRYPTED password will be decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally.

EXAMPLE

```
SM12DP2XA(config)# $sername 100ngine100ss privilege 15 password none
SM12DP2XA(config)# username BobB privilege 14 password unencrypted admin admin
SM12DP2XA(config)# username BobB privilege 13 password encrypted adminadminadmin123!@#
SM12DP2XA(config)#
```

Message: *% The UNENCRYPTED password is not accepted*

vlan

Configure VLAN parameters.

Syntax

vlan <vlan_list>

vlan ethertype s-custom-port <0x0600-0xffff>

vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } } group <grp_id>

Parameters

<vlan_list>	ISL VLAN IDs 1-4095
ethertype	Ether type for Custom S-ports
protocol	Protocol-based VLAN commands
s-custom-port	Custom S-ports configuration
<0x0600-0xffff>	Ether type (Range: 0x0600-0xffff>
eth2	Ethernet-based VLAN commands
<0x600-0xffff>	Ether Type(Range: 0x600 - 0xFFFF)
arp	Ether Type is ARP
ip	Ether Type is IP
ipx	Ether Type is IPX
at	Ether Type is AppleTalk
snap	SNAP-based VLAN group
<0x0-0xffffff>	SNAP OUI (Range 0x000000 - 0XFFFFFF)
rfc_1042	SNAP OUI is rfc_1042
snap_8021h	SNAP OUI is 8021h
<0x0-0xffff>	PID (Range: 0x0 - 0xFFFF)
llc	LLC-based VLAN group
<0x0-0xff>	DSAP (Range: 0x00 - 0xFF)
<0x0-0xff>	SSAP (Range: 0x00 - 0xFF)
group	Protocol-based VLAN group commands
<word16>	Group Name (Range: 1 - 16 characters)
do	To run exec commands in config mode
end	Go back to EXEC mode
exit	Exit from current mode
help	Description of the interactive help system
name	ASCII name of the VLAN

no	Negate

EXAMPLE

```
SM12DP2XA(config)# vlan 10-300
SM12DP2XA(config)# vlan ethertype s-custom-port 0x1111
SM12DP2XA(config)# vlan protocol eth2 arp group 123
SM12DP2XA(config)# vlan protocol llc 0xf0 0xf1 group Grp11
SM12DP2XA(config)
```

voice

Configure Voice VLAN parameters. 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. Voice VLAN enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured via its own GUI.

Syntax

voice vlan

voice vlan aging-time <aging_time>

voice vlan class { <traffic_class> | low | normal | medium | high }

voice vlan oui <oui> [description <description>]

voice vlan vid <vid>

Parameters

vlan	Vlan for voice traffic
aging-time	Set secure learning aging time
<10-10000000>	Aging time, 10-10000000 seconds
class	Set traffic class
<0-7>	Traffic class value
oui	OUI configuration
<oui>	OUI value
description	Set description for the OUI
<line32>	Description line
vid	Set VLAN ID
<vlan_id>	VLAN ID, 1-4095

EXAMPLE

```
SM12DP2XA(config)# vlan ethertype s-custom-port 0x1111
SM12DP2XA(config)# vlan protocol eth2 arp group 123
SM12DP2XA(config)# voice vlan aging-time 3333
SM12DP2XA(config)# voice vlan class 7
SM12DP2XA(config)# voice vlan vid 3333
SM12DP2XA(config)# voice vlan oui FC:EC:DA description Ubiquiti
SM12DP2XA(config)# do show voice vlan oui FC:EC:DA
Telephony OUI  Description
-------------  -----------
```

```
FC-EC-DA      Ubiquity
SM12DP2XA(config)#
```

web

Configure web privilege levels.

Syntax

web privilege group <group_name> level { [cro <configRoPriv>] [crw <configRwPriv>] [sro <statusRoPriv>] [srw <statusRwPriv>] }*1

Parameters

privilege	Web privilege			
group	Web privilege group			
CWORD	Aggregation	DHCP	DHCPv6_Client	DMS_client
	DMS_server	Debug	Diagnostics	IP
	IPMC_Snooping	Install_Wizard	LACP	LLDP
	Loop_Protect	MAC_Table	MRP	MVR
	Maintenance	NTP	Ports	Private_VLANs
	QoS	Rmirror	R_RING	SMTP
	Security	Spanning_Tree	System	TS_client
	TS_server	Trap_Event	Trouble_Shooting	UDLD
	UpnP	VCL	VLANs	VTUN
	Voice_VLAN	XXRP	Percepxion	sFlow
level	Web privilege group level			
cro	Configuration Read-only level			
crw	Configuration Read-write level			
sro	Status/Statistics Read-only level			
srw	Status/Statistics Read-write level			
<0-15>	privilege level			

EXAMPLE

```
SM12DP2XA(config)# web privilege group mvr level crw 15
SM12DP2XA(config)# web privilege group Install_Wizard level crw 15
SM12DP2XA(config)# web privilege group percepxion level crw 15
SM12DP2XA(config)# web privilege group percepxion level crw 15 cro 10 ?
    sro     Status/Statistics Read-only level
```

```
    srw     Status/Statistics Read-write level
    <cr>
SM12DP2XA(config)# web privilege group percepxion level crw 15 cro 10 srw 5
SM12DP2XA(config)#
```

Message: *% The privilege level of 'Status/Statistics Read-only' should be less than or equal to 'Status/Statistics Read-write*

no Commands

Negate a command or set its defaults in Config mode.

Table : configure – no Commands

Command	Function
aaa	Authentication, Authorization and Accounting
access	Access management
access-list	Access list
aggregation	Aggregation mode
banner	Define a login banner
clock	Configure time-of-day clock
command-history-log	Disable to Save Command 106ngine106 to Flash
dot1x	IEEE Standard for port-based Network Access Control
enable	Modify enable password parameters
exec-timeout	Auto-logout period
gvrp	Enable GVRP feature
hostname	Set system's network name
interface	Select an interface to configure
ip	Internet Protocol v4
ipmc	IPv4/IPv6 multicast configuration
ipv6	IPv6 configuration commands
lacp	LACP settings
lldp	LLDP configurations.
logging	System logging message
loop-protect	Loop protection configuration
mac	MAC table entries/configuration
map-api-key	Google Map API key
monitor	Monitoring different system events
mvr	Multicast VLAN Registration configuration
ntp	Configure NTP
port-security	Enable/disable port security globally.
privilege	Command privilege parameters
qos	Quality of Service
radius-server	Configure RADIUS
rmon	Remote Monitoring
sflow	Statistics flow.
snmp-server	Enable SNMP server
spanning-tree	STP Bridge
system	Set the system description
tacacs-server	Configure TACACS+
udld	Disable UDLD configurations on all fiber-optic ports
upnp	Set UpnP configuration
username	Establish User Name Authentication
vlan	VLAN commands
voice	Voice appliance attributes
web	Web

aaa

Negate Authentication, Authorization and Accounting.

Syntax

no aaa authentication login {console | telnet | ssh | http }

Parameters

authentication	Authentication
login	Login
console	Disable Console
http	Disable HTTP
ssh	Disable SSH
telnet	Disable Telnet

EXAMPLE

```
SM12DP2XA(config)# no aaa authentication login ssh
SM12DP2XA(config)# no aaa authentication login telnet
SM12DP2XA(config)#
```

access

Negate Access management

Syntax

no access management [<1~16>]

no access management

Parameters

management	Access management configuration
<1~16>	ID of access management entry

EXAMPLE

```
SM12DP2XA(config)# no access management
SM12DP2XA(config)#
```

access-list

Negate Access list

Syntax

no access-list ace <1~256>

Parameters

ace	Access list entry
<AceId : 1-256>	ACE ID

EXAMPLE

```
SM12DP2XA(config)# no access-list ace 1
SM12DP2XA(config)#
```

aggregation

Negate Aggregation mode

Syntax

no aggregation mode

Parameters

mode	Traffic distribution mode

EXAMPLE

```
SM12DP2XA(config)# no aggregation mode
SM12DP2XA(config)#
```

banner

Negate login banner

Syntax

no banner [motd]

no banner exec

no banner login

Parameters

exec	Set EXEC process creation banner
login	Set login banner
motd	Set Message of the Day banner

EXAMPLE

```
SM12DP2XA(config)# no banner login
SM12DP2XA(config)#
```

clock

Negate time-of-day clock

Syntax

no clock summer-time

no clock timezone

Parameters

summer-time	Configure summer (daylight savings) time
timezone	Configure time zone

EXAMPLE

```
SM12DP2XA(config)# no clock summer-time
SM12DP2XA(config)# no clock Timezone
SM12DP2XA(config)#
```

command-history-log

Disable to Save Command History to Flash.

Syntax

no command-history-log <cr>

Parameters

None

EXAMPLE

```
SM12DP2XA(config)# no command-history-log
SM12DP2XA(config)#
```

dot1x

Negate IEEE Standard for port-based Network Access Control

Syntax

no dot1x authentication timer inactivity

no dot1x authentication timer re-authenticate

no dot1x feature { [guest-vlan] [radius-qos] [radius-vlan] }

no dot1x guest-vlan [supplicant]

no dot1x max-reauth-req

no dot1x re-authentication

no dot1x system-auth-control

no dot1x timeout quiet-period

no dot1x timeout tx-period

Parameters

authentication	Authentication
feature	Globally enables/disables a dot1x feature functionality
guest-vlan	Guest VLAN
max-reauth-req	The number of time a Request Identity EAPOL frame is sent without response before considering entering the Guest VLAN.
re-authentication	Set Re-authentication state
system-auth-control	Set the global NAS state
timeout	timeout
timer	timer

inactivity	Time in seconds between check for activity on successfully authenticated MAC addresses.
re-authenticate	The period between re-authentication attempts in seconds
guest-vlan	Globally enables/disables state of guest-vlan
radius-qos	Globally enables/disables state of RADIUS-assigned QoS.
radius-vlan	Globally enables/disables state of RADIUS-assigned VLAN.
supplicant	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.
quiet-period	Time in seconds before a MAC-address that failed authentication gets a new authentication chance.
tx-period	the time between EAPOL retransmissions.

EXAMPLE

```
SM12DP2XA(config)# no dot1x authentication timer inactivity
SM12DP2XA(config)# no dot1x feature guest-vlan radius-qos radius-vlan
SM12DP2XA(config)# no dot1x guest-vlan supplicant
SM12DP2XA(config)# no dot1x max-reauth-req
SM12DP2XA(config)# no dot1x re-authentication
SM12DP2XA(config)# no dot1x system-auth-control
SM12DP2XA(config)# no dot1x timeout tx-period
SM12DP2XA(config)#
```

enable

Negate enable password parameters

Syntax

no enable password [level <1-15>]

no enable secret [0|5 { level <1-15> }]

Parameters

password	Assign the privileged level clear password
secret	Assign the privileged level secret
0	Specifies an UNENCRYPTED password will follow
5	Specifies an ENCRYPTED password will follow
level	Set exec level password
<1-15>	Level number

EXAMPLE

```
SM12DP2XA(config)# no enable secret level 15
SM12DP2XA(config)# no enable password level 15
SM12DP2XA(config)#
```

exec-timeout

No Auto-logout period.

Syntax

no exec-timeout autologout <cr>

Parameters

autologout autologout

<cr>

EXAMPLE

```
SM12DP2XA(config)# no exec-timeout autologout
SM12DP2XA(config)#
```

gvrp

No Enable GVRP functions.

Syntax

no gvrp

no gvrp max-vlans <maxvlans>

no gvrp time { [join-time <jointime>] [leave-time <leavetime>] [leave-all-time <leavealltime>] }*1

Parameters

max-vlans	Number of simultaneous VLANs that GVRP can control
time	Configure GARP protocol timer parameters. IEEE 802.1D-2004, clause 12.11.
<1-4095>	gvrp max-vlans
join-time	Set GARP protocol parameter JoinTime.
leave-all-time	Set GARP protocol parameter LeaveAllTime.
leave-time	Set GARP protocol parameter LeaveTime.
<1-20>	join-time in units of centi seconds. Range is 1-20. Default is 20.
<1000-5000>	leave-all-time in units of centi seconds Range is 1000-5000. Default is 1000.
<60-300>	leave-time in units of centi seconds. Range is 60-300. Default is 60.

<cr>

EXAMPLE

```
SM12DP2XA(config)# no gvrp max-vlans 200
SM12DP2XA(config)# no gvrp time leave-time 100
SM12DP2XA(config)#
```

hostname

Negate system's network name.

Syntax

no hostname

EXAMPLE

```
SM12DP2XA(config)# no hostname
SM12DP2XA(config)#
```

interface

No VLAN interface.

Syntax

no interface vlan < vlan_list >

Parameters

vlan	Vlan interface configurations
<vlan_list>	Vlan list

EXAMPLE

```
SM12DP2XA(config)# no interface vlan 10
SM12DP2XA(config)#
```

Ip

No IP network parameters.

Syntax

no ip arp inspection

no ip arp inspection entry interface Gigabitethernet <port_type_id> <vlan_id> <mac_ucast> <ipv4_ucast>

no ip arp inspection vlan <vlan_list> [logging]

no dhcp execluded-address [<ip_address> [<ip_address>]]

no dhcp pool <WORD>

no ip dhcp relay [information {option| policy }]

no ip dhcp server

no ip dhcp server per-port

no ip dhcp snooping

no ip dns proxy

no ip domain name

no ip helper-address

no ip igmp host-proxy [leave-proxy]

no ip igmp snooping

no ip igmp snooping vlan [<vlan_list>]

no ip igmp ssm-range

no ip igmp unknown-flooding

no ip name-server

no ip route <ipv4_addr> <ipv4_netmask> <ipv4_addr>

no ip routing

no ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mac_var>

no ip ssh

no ip verify source

Parameters

arp	Address Resolution Protocol
inspection	ARP inspection
entry	arp inspection entry
interface	arp inspection entry interface config
GigabitEthernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_id>	Port ID in the format of switch-no/port-no, 1/1-14 for Gigabitethernet, 1/1-2 for 10Gigabitethernet

<vlan_id>	Select a VLAN id to configure
<mac_ucast>	Select a MAC address to configure
<ipv4_ucast>	Select an IP Address to configure
vlan	arp inspection vlan setting
<vlan_list>	arp inspection vlan list
logging	ARP inspection vlan logging mode config
dhcp	Dynamic Host Configuration Protocol
execluded-address	Prevent DHCP from assigning certain address
<ip_address>	Low IP address and High IP address
<WORD>	Pool name in 32 characters
pool	Configure DHCP address pools
relay	DHCP relay agent configuration
server	enable DHCP server
snoping	DHCP snooping
information	DHCP information option(Option 82)
option	DHCP option
policy	Policy for handling the receiving DHCP packet already include the information option
snooping	DHCP snooping
dns	Domain Name System
proxy	DNS proxy service
helper-address	None.
http	Hypertext Transfer Protocol
secure-redirect	Secure HTTP web rediction
secure-server	Secure HTTP web server
igmp	Internet Group Management Protocol
host-proxy	IGMP proxy configuration
leave-proxy	IGMP proxy for leave configuration
snooping	Snooping IGMP
vlan	IGMP VLAN
<vlan_list>	VLAN identifier(s): VID
ssm-range	IPv4 address range of Source Specific Multicast
unknown-flooding	Flooding unregistered IPv4 multicast traffic
name-server	Domain Name System
Route	none
<ipv4_addr>	Network
<ipv4_netmask>	Netmask

<ipv4_gateway>	Gateway
routing	Disable routing for IPv4 and IPv6
source	source command
binding	ip source binding
interface	ip source binding entry interface config
Gigabitethernet	1 Gigabitethernet port
<port_type_id>	Port ID in the format of switch-no/port-no, ex., 1/1-14 for Gigabitethernet, 1/1-2 for 10Gigabitethernet
<vlan_id>	Select a VLAN id to configure
<ipv4_ucast>	Select an IP Address to configure
<ipv4_netmask>	Select a subnet mask to configure
<mac_ucast>	Select a MAC address to configure
ssh	Secure Shell
verify	verify command
source	verify source
per-port	Enable DHCP server per port
name	Define the default domain name

EXAMPLE

```
SM12DP2XA(config)# no ip arp inspection vlan 3 logging
SM12DP2XA(config)# no ip dhcp relay information option
SM12DP2XA(config)# no ip dhcp relay information option
SM12DP2XA(config)# no ip dns proxy
SM12DP2XA(config)# no ip helper-address
SM12DP2XA(config)# no ip http secure-redirect
SM12DP2XA(config)# no ip igmp snooping
SM12DP2XA(config)# no ip name-server
SM12DP2XA(config)# no ip routing
SM12DP2XA(config)# no ip ssh
SM12DP2XA(config)# no ip verify source
SM12DP2XA(config)#
```

ipmc

No IPv4/IPv6 multicast configuration.

Syntax

no ipmc profile <Profilename : word16>

no ipmc range <Entryname : word16>

Parameters

profile	IPMC profile configuration
<Profilename : word16>	Profile name in 16 char's
range	A range of IPv4/IPv6 multicast addresses for the profile
<Entryname : word16>	Range entry name in 16 char's

EXAMPLE

```
SM12DP2XA(config)# no ipmc profile
SM12DP2XA(config)#
```

ipv6

No IPv6 configuration commands .

Syntax

no ipv6 mld host-proxy [leave-proxy]

no ipv6 mld snooping

no ipv6 mld snooping [vlan <vlan_list>]

no ipv6 mld ssm-range

no ipv6 mld unknown-flooding

no ipv6 route <ipv6_subnet> { <ipv6_ucast> | interface vlan <vlan_id> <ipv6_linklocal> }

Parameters

mld	Multicasat Listener Discovery
host-proxy	MLD proxy configuration
leave-proxy	MLD proxy for leave configuration
snooping	Snooping MLD
vlan	MLD VLAN
<vlan_list>	VLAN identifier(s): VID
ssm-range	IPv6 address range of Source Specific Multicast
unknown-flooding	Flooding unregistered IPv6 multicast traffic
route	Configure static routes

<ipv6_subnet>	IPv6 prefix x:x::y/z
<ipv6_ucast>	IPv6 unicast address (except link-local address) of next-hop
interface	Select an interface to configure
vlan	VLAN Interface
<vlan_id>	VLAN identifier(s): VID
<ipv6_linklocal>	IPv6 link-local address of next-hop

EXAMPLE

```
SM12DP2XA(config)# no ipv6 mld snooping
SM12DP2XA(config)#
```

lacp

No LACP settings.

Syntax

no lacp system-priority <1-65535>

Parameters

system-priority	System priority
<1-65535>	Priority value, lower means higher priority

EXAMPLE

```
SM12DP2XA(config)# no lacp system-priority 10000
SM12DP2XA(config)#
```

lldp

No LLDP configurations.

Syntax

no lldp holdtime

no lldp med datum

no lldp med fast

no lldp med location-tlv altitude

no lldp med location-tlv civic-addr { country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code }

no lldp med location-tlv elin-addr

no lldp med location-tlv latitude

no lldp med location-tlv longitude

no lldp med media-vlan-policy <0~31>

no lldp reinit

no lldp timer

no lldp transmission-delay

Parameters

holdtime	Sets LLDP hold time (The neighbor switch will discard the LLDP information after “hold time” multiplied with “timer” seconds).
med	Media Endpoint Discovery.
reinit	Sets LLDP reinitialization delay.
timer	Sets LLDP TX interval (The time between each LLDP frame transmitted in seconds).
tlv-select	Which optional TLVs to transmit.
transmission-delay	Sets LLDP 120ngine120ssion-delay. LLDP transmission delay (the number of seconds that the transmission of LLDP frames will be delayed after LLDP configuration has changed).
datum	Set datum to default value.
fast	Set fast repeat count to default value.
location-tlv	LLDP-MED Location Type Length Value parameter.
media-vlan-policy	Use the media-vlan-policy to create a policy, which can be assigned to an interface.
altitude	Setting altitude to default.
civic-addr	Civic address information and postal information
elin-addr	Set elin address to default value.

latitude	Setting Latitude parameter to default.
longitude	Setting longitude to default.
additional-code	Additional code - Example: 1320300003.
additional-info	Additional location info - Example: South Wing.
apartment	Unit (Apartment, suite) - Example: Apt 42.
block	Neighbourhood, block.
building	Building (structure) - Example: Low Library.
city	City, township, shi (Japan) - Example: Copenhagen.
country	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
county	County, parish, gun (Japan), district.
district	City division, borough, city district, ward, chou (Japan).
floor	Floor - Example: 4.
house-no	House number - Example: 21.
house-no-suffix	House number suffix - Example: A, 1/2.
landmark	Landmark or vanity address - Example: Columbia University.
leading-street-direction	Leading street direction - Example: N.
name	Name (residence and office occupant) - Example: Flemming Jahn.
p-o-box	Post office box (P.O. BOX) - Example: 12345.
place-type	Place type - Example: Office.
postal-community-name	Postal community name - Example: Leonia.
room-number	Room number - Example: 450F.
state	National subdivisions (state, canton, region, province, prefecture).
street	Street - Example: Poppelvej.
street-suffix	Street suffix - Example: Ave, Platz.
trailing-street-suffix	Trailing street suffix - Example: SW.
zip-code	Postal/zip code - Example: 2791.
<0~31>	Policy to delete.

EXAMPLE

```
SM12DP2XA(config)# no lldp holdtime
SM12DP2XA(config)# no lldp med location-tlv civic-addr floor
SM12DP2XA(config)# no lldp reinit
SM12DP2XA(config)# no lldp timer
SM12DP2XA(config)# no lldp transmission-delay
SM12DP2XA(config)#
```

logging

No Syslog.

Syntax

no logging host

no logging on

Parameters

host	host
on	Enable syslog server

EXAMPLE

```
SM12DP2XA(config)# no logging host
SM12DP2XA(config)# no logging on
SM12DP2XA(config)#
```

loop-protect

No Loop protection configuration

Syntax

no loop-protect

no loop-protect shutdown-time

no loop-protect transmit-time

Parameters

shutdown-time	Loop protection shutdown time interval
transmit-time	Loop protection transmit time interval

EXAMPLE

```
SM12DP2XA(config)# no loop-protect shutdown-time
SM12DP2XA(config)# no loop-protect transmit-time
SM12DP2XA(config)#
```

mac

No MAC table entries/configuration

Syntax

no mac address-table aging-time [<0,10-1000000>]

no mac address-table static <mac_addr> vlan <vlan_id> interface {*|Gigabitethernet [<port_type_list>]}

Parameters

address-table	Mac table entries configuration/table
aging-time	Mac address aging time
<0,10-1000000>	Aging time in seconds, 0 disables aging
static	Static MAC address
<mac_addr>	48 bit MAC address: xx:xx:xx:xx:xx:xx
vlan	VLAN keyword
<vlan_id>	VLAN IDs 1-4095
interface	Select an interface to configure
Gigabitethernet	1 Gigabit Ethernet port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet

EXAMPLE

```
SM12DP2XA(config)# no mac address-table aging-time 10000
SM12DP2XA(config)#
```

map-api-key

Negate Google Maps API key.

Syntax

no map-api-key <cr>

Parameters

None

EXAMPLE

```
SM12DP2XA(config)# no map-api-key
SM12DP2XA(config)#
```

monitor

No monitor configuration.

Syntax

no monitor destination

no monitor source { interface Gigabitethernet <port_type_list> | cpu}

Parameters

Destination

source	The source port(s). That is the ports to be mirrored to the destination port.l
cpu	Mirror CPU traffic.
interface	Mirror Interface traffic.
Gigabitethernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet

EXAMPLE

```
SM12DP2XA(config)# no monitor destination
SM12DP2XA(config)# no monitor source cpu
SM12DP2XA(config)#
```

mvr

No Multicast VLAN Registration configuration.

Syntax

no mvr

no mvr name <word16> channel

no mvr name <word16> frame priority

no mvr name <word16> frame tagged

no mvr name <word16> igmp-address

no mvr name <word16> last-member-query-interval

no mvr name <word16> mode

no mvr vlan <vlan_list>

no mvr vlan <vlan_list> channel

no mvr vlan <vlan_list> frame priority

no mvr vlan <vlan_list> frame tagged

no mvr vlan <vlan_list> igmp-address

no mvr vlan <vlan_list> last-member-query-interval

no mvr vlan <vlan_list> mode [{channel | frame | igmp-address | last-member-query-interval}

Parameters

name	MVR multicast name
<word16>	MVR multicast VLAN name
channel	MVR channel configuration
frame	MVR control frame in TX
priority	Interface CoS priority
tagged	Tagged IGMP/MLD frames will be sent
igmp-address	MVR address configuration used in IGMP
last-member-query-interval	Last Member Query Interval in tenths of seconds
mode	MVR mode of operation
vlan	MVR multicast vlan
<vlan_list>	MVR multicast VLAN list

EXAMPLE

```
SM12DP2XA(config)# no mvr vlan 12 mode
SM12DP2XA(config)#
```

ntp

No NTP configuration.

Syntax

no ntp

no ntp server <1-5>

Parameters

server	Configure NTP server
<1-5>	index number

EXAMPLE

```
SM12DP2XA(config)# no ntp server 2
SM12DP2XA(config)#
```

port-security

Disable port security globally.

Syntax

no port-security

no port-security aging

no port-security aging time

Parameters

aging	Enable/disable port security aging.
time	Time in seconds between check for activity on learned MAC addresses.

EXAMPLE

```
SM12DP2XA(config)# no port-security aging time
SM12DP2XA(config)#
```

radius-server

No RADIUS server configurations.

Syntax

no radius-server attribute {32 | 4 | 95}

no radius-server deadtime

no radius-server host <host_name> [auth-port <auth_port>] [acct-port <acct_port>]

no radius-server key

no radius-server retransmit

no radius-server timeout

Parameters

Attribute	radius-server attribute (32, 4, 95)
deadtime	Time to stop using a RADIUS server that doesn't respond
host	Specify a RADIUS server
key	Set RADIUS encryption key
retransmit	Specify the number of retries to active server
timeout	Time to wait for a RADIUS server to reply

EXAMPLE

```
SM12DP2XA(config)# no radius-server attribute 4
SM12DP2XA(config)# no radius-server deadtime
SM12DP2XA(config)# no radius-server key
SM12DP2XA(config)# no radius-server retransmit
SM12DP2XA(config)# no radius-server timeout
SM12DP2XA(config)#
```

rmon

No Remote Monitoring.

Syntax

no rmon alarm <alarm : 1-65535>

no rmon event<event : 1-65535>

Parameters

alarm	Configure an RMON alarm
event	Configure an RMON event
<alarm : 1-65535>	Alarm entry ID
<event: 1-65535>	Event entry ID

EXAMPLE

```
SM12DP2XA(config)# no rmon alarm 1000
SM12DP2XA(config)#
```

sflow

No Statistics flow.

Syntax

no sflow agent-ip

no sflow collector-address

no sflow collector-port

no sflow max-datagram-size

no sflow timeout

Parameters

agent-ip	Sets the agent IP address used as agent-address in UDP datagrams to 127.0.0.1.
collector-address	Collector address
collector-port	Collector UDP port
max-datagram-size	Maximum datagram size.
timeout	Receiver timeout measured in seconds. The switch decrements the timeout once per second, and as long as it is non-zero, the receiver receives samples. Once the timeout reaches 0, the receiver and all its configuration is reset to defaults.

EXAMPLE

```
SM12DP2XA(config)# no sflow agent-ip
SM12DP2XA(config)# no sflow collector-address
```

```
SM12DP2XA(config)# no sflow collector-port
SM12DP2XA(config)# no sflow max-datagram-size
SM12DP2XA(config)# no sflow timeout
```

snmp-server

No SNMP server.

Syntax

no snmp-server

no snmp-server access <Groupname : word32> model { v1 | v2c | v3 | any } level { auth | noauth | priv }

no snmp-server community v2c

no snmp-server community v3 <Community : word127>

no snmp-server contact

no snmp-server 129ngine-id local

no snmp-server host <Conf : word32>

no snmp-server location

no snmp-server security-to-group model { v1 | v2c | v3 } name <Securityname : word32>

no snmp-server trap

no snmp-server user <Username : word32> engine-id <Engineid : word10-32>

no snmp-server version

no snmp-server view <Viewname : word32> <Oidsubtree : word255>

Parameters

access	access configuration
<: word32>	group name
model	security model
v1	v1 security model
v2c	v2c security model
v3	v3 security model
any	any security model
level	security level
auth	authNoPriv Security Level
noauth	noAuthNoPriv Security Level
priv	authPriv Security Level
community	Set the SNMP community
contact	Clear the SNMP server's contact string

130ngine-id	Set SNMP engine ID
host	Set SNMP host's configurations
location	Clear the SNMP server's location string
security-to-group	security-to-group configuration
trap	Set trap's configurations
user	user who can access SNMP server
version	Set the SNMP server's version
view	MIB view configuration
<Community >	SNMP community name
v2c	SNMPv2c
v3	SNMPv3
local	Set SNMP local engine ID
<ConfName : word32>	Name of the host configuration
model	security model
v1	v1 security model
v2c	v2c security model
v3	v3 security model
name	security user
<SecurityName : word32>	security user name
<Username : word32>	name of user
engine-id	engine ID
<Engineid : word10-32>	engine ID octet string
<Viewname : word32>	MIB view name
<Oidsubtree : word255>	MIB view OID

EXAMPLE

```
SM12DP2XA(config)# no snmp-server access 333 model any level auth
SM12DP2XA(config)# no snmp-server community v2c
SM12DP2XA(config)# no snmp-server engined-id local
SM12DP2XA(config)# no snmp-server host 333
SM12DP2XA(config)# no snmp-server location
SM12DP2XA(config)# no snmp-server security-to-group model v2c name 132
SM12DP2XA(config)# no snmp-server trap
SM12DP2XA(config)# no snmp-server version
SM12DP2XA(config)#
```

spanning-tree

No STP Bridge.

Syntax

no spanning-tree edge bpdu-filter

no spanning-tree edge bpdu-guard

no spanning-tree mode

no spanning-tree mst <instance> priority

no spanning-tree mst <instance> vlan

no spanning-tree mst forward-time

no spanning-tree mst max-age

no spanning-tree mst max-hops

no spanning-tree mst name

no spanning-tree recovery interval

no spanning-tree transmit hold-count

Parameters

edge	Edge ports
mode	STP protocol mode
mst	STP bridge instance
recovery	The error recovery timeout
transmit	BPDUs to transmit
bpdu-filter	Enable BPDU filter (stop BPDU tx/rx)
bpdu-guard	Enable BPDU guard
<Instance : 0-7>	instance 0-7 (CIST=0, MST2=1...)
priority	Priority of the instance
forward-time	Delay between port states
max-age	Max bridge age before timeout
max-hops	MSTP bridge max hop count
name	Name keyword
vlan	VLAN keyword
interval	The interval
hold-count	Max number of transmit BPDUs per sec
<Holdcount : 1-10>	1-10 per sec, 6 is default

EXAMPLE

```
SM12DP2XA(config)# no spanning-tree edge bpdu-filter
SM12DP2XA(config)# no spanning-tree mode
SM12DP2XA(config)# no spanning-tree mst max-age
SM12DP2XA(config)# no spanning-tree recovery interval
SM12DP2XA(config)# no spanning-tree transmit hold-count
SM12DP2XA(config)#
```

tacacs-server

No TACACS+ server configurations.

Syntax

no tacacs-server deadtime

no tacacs-server host <host_name> [port <port>]

no tacacs-server key

no tacacs-server timeout

Parameters

deadtime	Time to stop using a TACACS+ server that doesn't respond
host	Specify a TACACS+ server
< word1-255>	Host name or IP address
key	Set TACACS+ encryption key
timeout	Time to wait for a TACACS+ server to reply
key	Server specific key (overrides default)
port	TCP port for TACACS+ server
timeout	Time to wait for this TACACS+ server to reply (overrides default)
<Port : 0-65535>	TCP port number

EXAMPLE

```
SM12DP2XA(config)# no tacacs-server deadtime
SM12DP2XA(config)# no tacacs-server host 192.168.1.1 port 10000
SM12DP2XA(config)# no tacacs-server key
SM12DP2XA(config)# no tacacs-server timeout
SM12DP2XA(config)#
```

upnp

No UpnP configurations.

Syntax

no upnp

no upnp advertising-duration

no upnp ttl

Parameters

advertising-duration	Set advertising duration
ttl	Set TTL value

EXAMPLE

```
SM12DP2XA(config)# no upnp advertising-duration
SM12DP2XA(config)# no upnp ttl
SM12DP2XA(config)#
```

username

Negate User Name entry.

Syntax

no username <Username : word31>

Parameter

<Username : word31>	User name allows letters, numbers and underscores

EXAMPLE

```
SM12DP2XA(config)# no username admin
SM12DP2XA(config)#
```

vlan

No VLAN commands.

Syntax

no vlan protocol { { eth2 { <0x600-0xffff> | arp | ip | ipx | at } } | { snap { <0x0-0xffffff> | rfc_1042 | snap_8021h } <0x0-0xffff> } | { llc <0x0-0xff> <0x0-0xff> } } group <word16>

no vlan { [ethertype s-custom-port] | <vlan_list> }

Parameters

protocol	Protocol-based VLAN commands
eth2	Ethernet-based VLAN commands
<0x600-0xffff>	Ether Type(Range: 0x600 - 0xFFFF)
arp	Ether Type is ARP
ip	Ether Type is IP
ipx	Ether Type is IPX
at	Ether Type is AppleTalk
snap	SNAP-based VLAN group
<0x0-0xffffff>	SNAP OUI (Range 0x000000 - 0XFFFFFF)
rfc_1042	SNAP OUI is rfc_1042
snap_8021h	SNAP OUI is 8021h
<0x0-0xffff>	PID (Range: 0x0 - 0xFFFF)
llc	LLC-based VLAN group
<0x0-0xff>	DSAP (Range: 0x00 - 0xFF)
<0x0-0xff>	SSAP (Range: 0x00 - 0xFF)
group	Protocol-based VLAN group commands
<word16>	Group Name (Range: 1 - 16 characters)
<vlan_list>	Vlan list
ethertype	
s-custom-port	

EXAMPLE

```
SM12DP2XA(config)# no vlan 3
SM12DP2XA(config)# no vlan ethertype s-custom-port
SM12DP2XA(config)#
```

voice

No Voice appliance parameters.

Syntax

no voice vlan

no voice vlan aging-time

no voice vlan class

no voice vlan oui <oui>

no voice vlan vid

Parameters

vlan	Vlan for voice traffic
aging-time	Set secure learning aging time
class	Set traffic class
oui	OUI configuration
<oui>	Traffice class value
vid	Set VLAN ID

EXAMPLE

```
SM12DP2XA(config)# no voice vlan vid
SM12DP2XA(config)# no voice vlan class
SM12DP2XA(config)# no voice vlan aging-time
SM12DP2XA(config)#
```

web

No Web privilege.

Syntax

no web privilege group [<group_name>] level

Parameters

privilege	Web privilege			
group	Web privilege group			
<CWORD>	Valid words are:			
	Aggregation	DHCP	DHCPv6_Client	DMS_client
	DMS_server	Debug	Diagnostics	IP
	IPMC_Snooping	Install_Wizard	LACP	LLDP
	Loop_Protect	MAC_Table	MRP	MVR
	Maintenance	NTP	Ports	Private_VLANs
	QoS	Rmirror	R_RING	SMTP
	Security	Spanning_Tree	System	TS_client
	TS_server	Trap_Event	Trouble_Shooting	UDLD
	UpnP	VCL	VLANs	VTUN
	Voice_VLAN	XXRP	level	percepxion
	sFlow			
level	Web privilege group level			

EXAMPLE

```
SM12DP2XA(config)# no web privilege group LACP level
SM12DP2XA(config)# no web privilege group UpnP level
SM12DP2XA(config)# no web privilege group level
SM12DP2XA(config)#
```

qos

Table : configure – qos Commands

Command	Function
map	Global QoS Map/Table
qce	QoS Control Entry
storm	Storm policer
wred	Weighted Random Early Discard

map

Configure Global QoS Map/Table parameters.

Syntax

qos map cos-dscp <0~7> dpl <dpl : 0~1> dscp { <DscpNum : 0-63> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

qos map dscp-classify { <dscpNum : 0~63> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

qos map dscp-cos { < dscpNum : 0~63> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } cos <Cos : 0-7> dpl <dpl>

qos map dscp-egress-translation { < DscpNum : 0~63> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } <Dpl : 0~1> to { <Dscpnum : 0-63> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

qos map dscp-ingress-translation { < DscpNum : 0~63> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } to { < DscpNum : 0-63> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Parameters

cos-dscp	Map for cos to dscp
dscp-classify	Map for dscp classify enable
dscp-cos	Map for dscp to cos
dscp-egress-translation	Map for dscp egress translation
dscp-ingress-translation	Map for dscp ingress translation
dpl	Specify drop precedence level
<Dpl : 0~1>	Specific drop precedence level or range
dscp	Specify DSCP
<DscpNum : 0-63>	Specific DSCP

cos	Specify class of QoS
<Cos : 0-7>	Specific class of QoS
af11	Assured Forwarding PHB AF11(DSCP 10)
af12	Assured Forwarding PHB AF12(DSCP 12)
af13	Assured Forwarding PHB AF13(DSCP 14)
af21	Assured Forwarding PHB AF21(DSCP 18)
af22	Assured Forwarding PHB AF22(DSCP 20)
af23	Assured Forwarding PHB AF23(DSCP 22)
af31	Assured Forwarding PHB AF31(DSCP 26)
af32	Assured Forwarding PHB AF32(DSCP 28)
af33	Assured Forwarding PHB AF33(DSCP 30)
af41	Assured Forwarding PHB AF41(DSCP 34)
af42	Assured Forwarding PHB AF42(DSCP 36)
af43	Assured Forwarding PHB AF43(DSCP 38)
be	Default PHB(DSCP 0) for best effort traffic
cs1	Class Selector PHB CS1 precedence 1(DSCP 8)
cs2	Class Selector PHB CS2 precedence 2(DSCP 16)
cs3	Class Selector PHB CS3 precedence 3(DSCP 24)
cs4	Class Selector PHB CS4 precedence 4(DSCP 32)
cs5	Class Selector PHB CS5 precedence 5(DSCP 40)
cs6	Class Selector PHB CS6 precedence 6(DSCP 48)
cs7	Class Selector PHB CS7 precedence 7(DSCP 56)
ef	Expedited Forwarding PHB(DSCP 46)
va	Voice Admit PHB(DSCP 44)

EXAMPLE

```
SM12DP2XA(config)# qos map cos-dscp 5 dpl 1 dscp 20
SM12DP2XA(config)# qos qce 1 action policy 0
SM12DP2XA(config)# qos storm broadcast 9000
SM12DP2XA(config)# qos wred group 1 queue 0 dpl 1 min-fl 20 max 60 fill-level
SM12DP2XA(config)#
```

qce

Configure QoS Control Entries. A QoS Control List (QCL) is made up of QCEs. A 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 4 different QoS classes: “Low”, “Normal”, “Medium”, and “High” for individual application. The maximum number of QCEs is 256 on each switch.

Syntax

qos qce refresh

qos qce { [update] } <Id : 1-256> [{ next <Id : 1-256> } | last] [ingress interface *|Gigabitethernet] [tag { tagged | untagged | any }] [vid { <vlan_list> | any }] [pcp { <pcp> | any }] [dei { <Dpl : 0-1> | any }] [smac { <mac_addr> | <oui> | any }] [dmac-type { unicast | multicast | broadcast | any }] [frametype { any | { etype [{ <0x600-0x7ff,0x801-0x86dc,0x86de-0xffff> | any }] } | { llc [dsap { <0-0xff> | any }] [ssap { <0-0xff> | any }] [control { <0-0xff> | any }] } | { snap [{ <0-0xffff> | any }] } | { ipv4 [proto { <0-255> | tcp | udp | any }] [sip { <ipv4_subnet> | any }] [dscp { <0~63> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any }] [frag { yes | no | any }] [sport { <0~65535> | any }] [dport { <0~65535> | any }] } | { ipv6 [proto { <0-255> | tcp | udp | any }] [sip { <ipv4_subnet> | any }] [dscp { <0~63> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any }] [sport { <0~65535> | any }] [dport { <0~65535> | any }] } }] [action { [cos { <0-7> | default }] [dpl { <0-1> | default }] [dscp { <0-63> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | default }] }]

Parameters

<Id : 1-256>	QCE ID
refresh	Refresh QCE tables in hardware
update	Update an existing QCE
action	Specify action
dei	Specify DEI (Drop Eligible Indicator)
dmac-type	Specify DMAC type
frametype	Specify frame type
ingress	Ingress interfaces
last	Place QCE at the end
next	Place QCE before the next QCE ID
pcp	Specify PCP (Priority Code Point)
smac	Specify SMAC. If ‘qos qce dmac-dip’ is set, this parameter specifies the DMAC
tag	Specify tag options
vid	Specify VLAN ID

cos	Specify class of service
dpl	Specify drop precedence level
dscp	Specify DSCP
cos	Specify class of service
<Cos : 0-7>	Specific class of service
default	Keep default class of service
<Dpl : 0-1>	Specific drop precedence level
default	Keep default drop precedence level
<Dscp : 0-63>	Specific DSCP
af11	Assured Forwarding PHB AF11(DSCP 10)
af12	Assured Forwarding PHB AF12(DSCP 12)
af13	Assured Forwarding PHB AF13(DSCP 14)
af21	Assured Forwarding PHB AF21(DSCP 18)
af22	Assured Forwarding PHB AF22(DSCP 20)
af23	Assured Forwarding PHB AF23(DSCP 22)
af31	Assured Forwarding PHB AF31(DSCP 26)
af32	Assured Forwarding PHB AF32(DSCP 28)
af33	Assured Forwarding PHB AF33(DSCP 30)
af41	Assured Forwarding PHB AF41(DSCP 34)
af42	Assured Forwarding PHB AF42(DSCP 36)
af43	Assured Forwarding PHB AF43(DSCP 38)
be	Default PHB(DSCP 0) for best effort traffic
cs1	Class Selector PHB CS1 precedence 1(DSCP 8)
cs2	Class Selector PHB CS2 precedence 2(DSCP 16)
cs3	Class Selector PHB CS3 precedence 3(DSCP 24)
cs4	Class Selector PHB CS4 precedence 4(DSCP 32)
cs5	Class Selector PHB CS5 precedence 5(DSCP 40)
cs6	Class Selector PHB CS6 precedence 6(DSCP 48)
cs7	Class Selector PHB CS7 precedence 7(DSCP 56)
default	Keep default DSCP
ef	Expedited Forwarding PHB(DSCP 46)
va	Voice Admit PHB(DSCP 44)
any	Any
broadcast	Broadcast
multicast	Multicast
unicast	Unicast

etype	Ethernet frames
ipv4	IPv4 frames
ipv6	IPv6 frames
llc	LLC frames
snap	SNAP frames
<Etype : 0x600-0x7ff,0x801-0x86dc,0x86de-0xffff>	Specific EtherType
interface	Interfaces
<Next : 1-256>	The next QCE ID
<Pcp : pcp>	Specific PCP (0-7) or range (0-1, 2-3, 4-5, 6-7, 0-3 or 4-7)
<Smac : mac_addr>	Specific SMAC (XX-XX-XX-XX-XX-XX)
tagged	Tagged frames only
untagged	Untagges frames only
<Vid : vlan_list>	Specific VLAN ID or range
interface	Interfaces
Gigabitethernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<PORT_LIST>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet

EXAMPLE

```
SM12DP2XA(config)# qos map cos-dscp 5 dpl 1 dscp 20
SM12DP2XA(config)# qos qce 1 action cos 0 tag vid any
SM12DP2XA(config)# qos qce refresh
SM12DP2XA(config)# qos qce update 1
SM12DP2XA(config)#
```

storm

Configure QoS storm parameters. There is a unicast storm policer, multicast storm policer, and a broadcast storm policer. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

Syntax

qos storm { unicast | multicast | broadcast } <rate> [fps | kfps | kbps | mbps]

Parameters

broadcast	Police broadcast frames
multicast	Police multicast frames
unicast	Police unicast frames
<1-13128147>	Policer rate (default fps). Internally rounded up to the nearest value supported by the storm policer.
fps	Unit is frames per second (default)
kbps	Unit is kilobits per second
kfps	Unit is kiloframes per second
mbps	Unit is Megabits per second
<cr>	

EXAMPLE

```
SM12DP2XA(config)# qos storm unicast 12345678 ?
    fps     Unit is frames per second (default)
    kbps    Unit is kilobits per second
    kfps    Unit is kiloframes per second
    mbps    Unit is Megabits per second
    <cr>
SM12DP2XA(config)# qos storm unicast 12345678
SM12DP2XA(config)# qos storm broadcast 50000 kbps
SM12DP2XA(config)#
```

wred

Configure Weighted Random Early Detection (WRED) parameters. 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 switch.

Syntax

qos wred queue <queue> min-th <min_th> mdp-1 <mdp_1> mdp-2 <mdp_2> mdp-3 <mdp_3>

Parameters

queue	Specify queue
<Queue : 0~5>	Specific queue or range
<MinTh : 0-100>	Specific minimum threshold in percent
mdp-1	Specify drop probability for drop precedence level 1
<Mdp1 : 0-100>	Specific drop probability in percent
mdp-2	Specify drop probability for drop precedence level 2
<Mdp2 : 0-100>	Specific drop probability in percent
mdp-3	Specify drop probability for drop precedence level 3
<Mdp3 : 0-100>	Specific drop probability in percentunicast

EXAMPLE

```
SM12DP2XA(config)# qos map cos-dscp 5 dpl 1 dscp 20
SM12DP2XA(config)# qos wred group 1 queue 4 dpl 2 min-fl 25 max 75 fill-level
SM12DP2XA(config)# qos wred group 2 queue 2 dpl 2 min-fl 50 max 99
SM12DP2XA(config)#
```

snmp-server

Configure SNMP server parameters. Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage managed devices equipped with an SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP protocol is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. The SNMP agent running on the switch responds the requests issued by an SNMP manager.

Table : configure snmp-server Commands

Command	Function
access	access configuration
community	Set the SNMP community
contact	Set the SNMP server's contact string
engine-id	Set SNMP engine ID
host	Set SNMP host's configurations
location	Set the SNMP server's location string
security-to-group	security-to-group configuration
trap	Set trap's configurations
user	Set the SNMPv3 user's configurations
version	Set the SNMP server's version
view	MIB view configuration

access

SNMP server access configuration.

Syntax

snmp-server access <group_name> model { v1 | v2c | v3 | any } level { auth | noauth | priv } [read <view_name>]

[write <write_name>]

Parameters

<GroupName : word32>	group name
model	security model
any	any security model
v1	v1 security model
v2c	v2c security model
v3	v3 security model
level	security level
auth	authNoPriv Security Level
noauth	noAuthNoPriv Security Level
priv	authPriv Security Level
read	specify a read view for the group
write	specify a write view for the group
<word32>	read view name
<word32>	write view name

EXAMPLE

```
SM12DP2XA(config)# snmp-server access text model v2c level noauth write text
SM12DP2XA(config)#
```

community

Set the SNMP community.

Syntax

snmp-server community v2c <comm> [ro | rw]

snmp-server community v2c readcommunity { enable | disable }

snmp-server community v2c writecommunity { enable | disable }

snmp-server community v3 <v3_comm> [<v_ipv4_addr> <v_ipv4_netmask>]

snmp-server community writecommunity { enable | disable }

Parameters

v2c	SNMP version
v3	SNMPv3
writecommunity	SNMP server WriteCommunity
<word255>	Community word
ro	Read only
rw	Read write
<ipv4_addr>	IPv4 address
<ipv4_netmask>	IPv4 netmask
disable	Disable SNMP server WriteCommunity
enable	Enable SNMP server WriteCommunity

EXAMPLE

```
SM12DP2XA(config)# snmp-server community v2c text
SM12DP2XA(config)# snmp-server community v3 MnBC 2.3.4.5 255.255.255.0
SM12DP2XA(config)# snmp-server community writecommunity enable
SM12DP2XA(config)# exit
SM12DP2XA# show snmp community v3
Community   : MnBC
Source IP   : 2.3.4.5
Source Mask : 255.255.255.0

Community   : public
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0

Community   : private
Source IP   : 0.0.0.0
```

```
Source Mask : 0.0.0.0


SM12DP2XA#
```

contact

Set the SNMP server's contact string.

Syntax

snmp-server contact <v_line255>

Parameters

contact	Set the SNMP server's contact string
<line255>	contact string

EXAMPLE

```
SM12DP2XA(config)# snmp-server contact BobB
SM12DP2XA(config)#
```

engine-id

Set SNMP engine ID.

Syntax

snmp-server engine-id local <Engineid : word10-32>

Parameters

local	Set SNMP local engine ID
<word10-64>	local engine ID

EXAMPLE

```
SM12DP2XA(config)# snmp-server engine-id local 1234567891
SM12DP2XA(config)#
```

host

Set SNMP host's configurations.

Syntax

snmp-server host <conf_name>

Parameter

<word32> Name of the host configuration

EXAMPLE

```
SM12DP2XA(config)# snmp-server host text
SM12DP2XA(config)#
```

location

Set the SNMP server's location string.

Syntax

snmp-server location <v_line255>

Parameter

<line255> location string

EXAMPLE

```
SM12DP2XA(config)# snmp-server location 55345
SM12DP2XA(config)#
```

security-to-group

SNMP security-to-group configuration.

Syntax

snmp-server security-to-group model { v1 | v2c | v3 } name <security_name> group <group_name>

Parameters

model	security model
v1	v1 security model
v2c	v2c security model
v3	v3 security model
name	security user
<word32>	security user name
group	security group
< word32>	security group name

EXAMPLE

```
SM12DP2XA(config)# $ecurity-to-group model v2c name text group text
SM12DP2XA(config)#
```

trap

Set SNMP trap's configurations.

Syntax

snmp-server trap

EXAMPLE

```
SM12DP2XA(config)# snmp-server trap
SM12DP2XA(config)#
```

user

Set the SNMPv3 user's parameters.

Syntax

snmp-server user <username> engine-id <engineID> [{ md5 { <md5_passwd> | { encrypted <md5_passwd_encrypt> } } | sha { <sha_passwd> | { encrypted <sha_passwd_encrypt> } } } [priv { des | aes } { <priv_passwd> | { encrypted <priv_passwd_encrypt> } }]]

Parameters

<word32>	Username
engine-id	engine ID
<word10-32>	Engine ID octet string
md5	Set MD5 protocol
<word8-32>	MD5 password
sha	Set SHA protocol
<word8-40>	SHA password
priv	Set Privacy
aes	Set AES protocol
des	Set DES protocol
<word8-32>	Set privacy password
<word8-32>	MD5 unencrypted password
encrypted	Specifies an ENCRYPTED password will follow.
<word8-84>	MD5 encrypted password
<word8-32>	Privacy unencrypted password
<word8-84>	Set privacy password

EXAMPLE

```
SM12DP2XA(config)# $ne-id 1234567891 md5 12345678 priv aes 12345678
SM12DP2XA(config)# snmp-server user BobB engine-id 1234567812345678 md5 semaphoreHJK
```

Messages:

% The UNENCRYPTED password is not accepted

The format of 'Engine ID' may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

% The same user entry already exists

version

Set the SNMP server's version.

Syntax

snmp-server version { v1 | v2c | v3 }

Parameters

v1 SNMPv1

v2c SNMPv2c

v3 SNMPv3

EXAMPLE

```
SM12DP2XA(config)# snmp-server version v2c
SM12DP2XA(config)# snmp-server version v3
SM12DP2XA(config)#
```

view

SNMP server MIB view configuration.

Syntax

snmp-server view <view_name> <oid_subtree> { include | exclude }

Parameters

<word32> MIB view name

<word255> MIB view OID

exclude Excluded type from the view

include Ixcluded type from the view

EXAMPLE

```
SM12DP2XA(config)# snmp-server view text .1 include
SM12DP2XA(config)# snmp-server view text .22 include
SM12DP2XA(config)# snmp-server view text .22 exclude
SM12DP2XA(config)#
```

spanning-tree

Configure Spanning Tree Protocol (STP) parameters.

Table : Configure spanning-tree Commands

Command	Function
aggregation	Aggregation mode
edge	Edge ports
mode	STP protocol mode
mst	STP bridge instance
recovery	The error recovery timeout
transmit	BPDUs to transmit

aggregation

Configure Spanning Tree Protocol Aggregation mode.

Syntax

spanning-tree aggregation <cr>

spanning-tree

spanning-tree auto-edge

spanning-tree bpdu-guard

spanning-tree edge

spanning-tree link-type { point-to-point | shared | auto }

spanning-tree mst <instance> cost { <cost> | auto }

spanning-tree mst <instance> port-priority <prio>

spanning-tree restricted-role

spanning-tree restricted-tcn

Parameters

do	To run exec commands in config mode
end	Go back to EXEC mode
exit	Exit from current mode
help	Description of the interactive help system
no	Negate a command or set its defaults
spanning-tree	Spanning Tree protocol
auto-edge	Auto detect edge status
bpdu-guard	Enable/disable BPDU guard

edge	Edge port
link-type	Port link-type
mst	STP bridge instance
restricted-role	Port role is restricted (never root port)
restricted-tcn	Restrict topology change notifications
auto	Auto detect
point-to-point	Forced to point-to-point
shared	Forced to Shared
<0-7>	instance 0-7 (CIST=0, MST2=1...)
cost	STP Cost of this port
port-priority	STP priority of this port
<1-200000000>	Cost range
auto	Use auto cost
<0-240>	Range (lower higher priority)

EXAMPLE

```
SM12DP2XA(config)# spanning-tree aggregation
SM12DP2XA(config-stp-aggr)# spanning-tree
SM12DP2XA(config-stp-aggr)# spanning-tree auto-edge
SM12DP2XA(config-stp-aggr)# spanning-tree bpdu-guard
SM12DP2XA(config-stp-aggr)# spanning-tree edge
SM12DP2XA(config-stp-aggr)# spanning-tree link-type point-to-point
SM12DP2XA(config-stp-aggr)# spanning-tree mst 0 cost 50000
SM12DP2XA(config-stp-aggr)# spanning-tree restricted-role
SM12DP2XA(config-stp-aggr)# spanning-tree restricted-tcn
SM12DP2XA(config-stp-aggr)# exit
SM12DP2XA(config)#
```

Messages: *Could not set MSTP port conf*

edge

Configure STP Edge ports.

Syntax

spanning-tree edge bpdu-filter

spanning-tree edge bpdu-guard

Parameters

bpdu-filter Enable BPDU filter (stop BPDU tx/rx)

bpdu-guard Enable BPDU guard

EXAMPLE

```
SM12DP2XA(config)# spanning-tree edge bpdu-filter
SM12DP2XA(config)# spanning-tree edge bpdu-guard
SM12DP2XA(config)#
```

mode

Set Spanning Tree protocol mode.

Syntax

spanning-tree mode { stp | rstp | mstp }

Parameters

mstp Multiple Spanning Tree (802.1s)

rstp Rapid Spanning Tree (802.1w)

stp 802.1D Spanning Tree

EXAMPLE

```
SM12DP2XA(config)# spanning-tree mode mstp
SM12DP2XA(config)# spanning-tree mode rstp
SM12DP2XA(config)# spanning-tree mode stp
SM12DP2XA(config)#
```

mst

Configure STP bridge instance.

Syntax

spanning-tree mst <instance> priority <prio>

spanning-tree mst <instance> vlan <v_vlan_list>

spanning-tree mst forward-time <fwdtime>

spanning-tree mst hello-time <hellotime>

spanning-tree mst max-age <maxage> [forward-time <fwdtime>]

spanning-tree mst max-hops <maxhops>

spanning-tree mst name <name> revision <v_0_to_65535>

Parameters

<Instance : 0-7>	instance 0-7 (CIST=0, MST2=1...)
forward-time	Delay between port states
max-age	Max bridge age before timeout
hello-time	MSTP bridge hello time
max-hops	MSTP bridge max hop count
name	Name keyword
priority	Priority of the instance
vlan	VLAN keyword
<0-61440>	Range in seconds
<vlan_list>	Range of VLANs
< 4-30>	Range in seconds
<6-40>	Range in seconds
<6-40>	Hop count range
<word32>	Name of the bridge
revision	Revision keyword
<0-65535>	Revision number

EXAMPLE

```
SM12DP2XA(config)# spanning-tree mst 7 vlan 10
SM12DP2XA(config)# spanning-tree mst hello-time 4
SM12DP2XA(config)#
```

Messages: *Could not set MSTP bridge parameters*

STP bridge priority must be one of 0/4096/8192/12288/.../53248/57344/61440 i.e. divisable by 4096.

recovery

Configure Spanning Tree error recovery intertval.

Syntax

spanning-tree recovery interval <Interval : 30-86400>

Parameters

interval	The interval
<30-86400>	Range in seconds

EXAMPLE

```
SM12DP2XA(config)# spanning-tree recovery interval 50
SM12DP2XA(config)#
```

transmit

BPDUs to transmit.

Syntax

spanning-tree transmit hold-count <Holdcount : 1-10>

Parameters

hold-count	Max number of transmit BPDUs per second
<1-10>	1-10 per second, 6 is default

EXAMPLE

```
SM12DP2XA(config)# spanning-tree transmit hold-count 5
SM12DP2XA(config)#
```

7. Interface Config Mode Commands

To view the configurable interfaces, type `interface ?` at the config mode prompt.

```
SM12DP2XA(config)# interface ?
    *                  All switches or All ports
    GigabitEthernet     1 Gigabit Ethernet Port
    10GigabitEthernet   10 Gigabit Ethernet Port
    vlan               VLAN interface configurations
SM12DP2XA (config)# interface *
SM12DP2XA (config-if)#
```

To enter Interface Config mode, type `interface <interface>` at the config mode prompt.

Example:

```
SM12DP2XA (config)# interface GigabitEthernet ½
SM12DP2XA (config-if)#
```

Interface Config Mode Commands (Switch / Ports)

access-list	Access list
aggregation	Create an aggregation
broadcast-storm-protection	Broadcast Storm Protection
debug	Debugging functions
description	Configures port description
do	To run exec commands in config mode
dot1x	IEEE Standard for port-based Network Access Control
duplex	Interface duplex
end	Go back to EXEC mode
excessive-restart	Restart backoff algorithm after 16 collisions (No excessive-restart means discard frame after 16 collisions)
exit	Exit from current mode
flowcontrol	Traffic flow control. Standard and priority flowcontrol cannot both be enabled or PFC not supported.
frame-length-check	Drop frames with mismatch between EtherType/Length field and actual payload size.
gvrp	Enable GVRP on interface or interfaces
help	Description of the interactive help system
ip	Internet Protocol

ipv6	IPv6 configuration commands
lacp	Enable LACP on this interface
lldp	LLDP configurations.
loop-protect	Loop protection configuration on port
mac	MAC keyword
mtu	Maximum transmission unit
mvr	Multicast VLAN Registration configuration
no	Negate a command or set its defaults
platform	Platform debug
port-security	Enable/disable port security per interface.
priority-flowcontrol	Priority Flow Control (802.1Qbb). Standard and priority flowcontrol cannot both be enabled or PFC not supported.
pvlan	Private VLAN
qos	Quality of Service
rmon	Configure Remote Monitoring on an interface
sflow	Statistics flow.
shutdown	Shutdown of the interface.
spanning-tree	Spanning Tree protocol

speed	Configures interface speed. If you use 10, 100, or 1000 keywords with the auto keyword the port will only advertise the specified speeds.
switchport	Switching mode characteristics
udld	UDLD configurations.
inspection	ARP inspection
check-vlan	ARP inspection VLAN mode configuration
logging	ARP inspection logging mode configuration
trust	ARP inspection trust configuration
all	log all entries
deny	log denied entries
permit	log permitted entries
snooping	DHCP snooping
trust	DHCP Snooping trust configuration
action	Access list action
logging	Logging frame information. 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.
mirror	Mirror frame to destination mirror port
policy	Policy
port-state	Re-enable shutdown port that was shutdown by access-list module
rate-limiter	Rate limiter
redirect	Redirect frame to specific port
shutdown	Shutdown incoming port. The shutdown feature only works when the packet length is less than 1518 (without VLAN tags)
deny	Deny as Access list action
permit	Permit as Access list action
<0-255>	Policy ID
<1-16>	Rate limiter ID
interface	Select an interface to configure
*	All switches or All ports
GigabitEthernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14
<port_type_list>	Port list in 1/1-2
filter	Access control on IGMP multicast group registration
immediate-leave	Immediate leave configuration

max-groups	IGMP group throttling configuration
mrouter	Multicast router port configuration
<word16>	Profile name in 16 char's
<1-10>	Maximum number of IGMP group registration
source	verify source
limit	limit command
<0-2>	the number of limit
<cr>	

Syntax:

access-list action { permit | deny }

access-list logging

access-list mirror

access-list policy <policy_id>

access-list port-state

access-list rate-limiter <rate_limiter_id>

access-list shutdown

access-list { redirect } interface { <port_type> <port_type_id> | (<port_type> [<port_type_list>]) }

aggregation group <v_uint>

broadcast-storm-protection

broadcast-storm-protection action { shutdown | log | both }

broadcast-storm-protection pps <v_0_to_1000000>

broadcast-storm-protection timer <v_0_to_65535>

description <description>

do <command>

dot1x guest-vlan

dot1x port-control { force-authorized | force-unauthorized | auto | single | multi | mac-based | mac-auth-bypass }

dot1x radius-qos

dot1x radius-vlan

dot1x re-authenticate

duplex { half | full | auto [half | full] }

end

excessive-restart

exit

flowcontrol { on | off }

frame-length-check

gvrp

help

ip arp inspection check-vlan

ip arp inspection logging { deny | permit | all }

ip arp inspection trust

ip dhcp snooping trust

ip igmp snooping filter <profile_name>

ip igmp snooping immediate-leave

ip igmp snooping max-groups <throttling>

ip igmp snooping mrouter

ip verify source

ip verify source limit <cnt_var>

ipv6 mld snooping filter <profile_name>

ipv6 mld snooping immediate-leave

ipv6 mld snooping max-groups <throttling>

ipv6 mld snooping mrouter

lacp

lacp key { <v_1_to_65535> | auto }

lacp port-priority <v_1_to_65535>

lacp role { active | passive }

lacp timeout { fast | slow }

lldp cdp-aware

lldp med media-vlan policy-list <v_range_list>

lldp med transmit-tlv [capabilities] [location] [network-policy] [poe]

lldp med type { connectivity | end-point }

lldp receive

lldp tlv-select { management-address | port-description | system-capabilities |system-description | system-name }

lldp transmit

loop-protect

loop-protect action { [shutdown] [log] }*1

loop-protect tx-mode

mac address-table learning [secure]

mtu <max_length>

mvr immediate-leave

mvr name <mvr_name> type { source | receiver }

mvr vlan <v_vlan_list> type { source | receiver }

no access-list logging

no access-list mirror

no access-list policy

no access-list port-state

no access-list rate-limiter

no access-list redirect

no access-list shutdown

no aggregation group
no broadcast-storm-protection
no broadcast-storm-protection action
no broadcast-storm-protection pps
no broadcast-storm-protection timer
no debug phy loopback [near | far]
no description
no dot1x guest-vlan
no dot1x port-control
no dot1x radius-qos
no dot1x radius-vlan
no duplex
no excessive-restart
no flowcontrol
no frame-length-check
no gvrp
no ip arp inspection check-vlan
no ip arp inspection logging
no ip arp inspection trust
no ip dhcp snooping trust
no ip igmp snooping filter
no ip igmp snooping immediate-leave
no ip igmp snooping max-groups
no ip igmp snooping mrouter
no ip verify source
no ip verify source limit
no ipv6 mld snooping filter
no ipv6 mld snooping immediate-leave
no ipv6 mld snooping max-groups
no ipv6 mld snooping mrouter
no lacp
no lacp key { <v_1_to_65535> | auto }
no lacp port-priority <v_1_to_65535>
no lacp role { active | passive }
no lacp timeout { fast | slow }
no lldp cdp-aware

no lldp med media-vlan policy-list [<v_range_list>]

no lldp med transmit-tlv [capabilities] [location] [network-policy] [poe]

no lldp med type

no lldp receive

no lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name }

no lldp transmit

no loop-protect

no loop-protect action

no loop-protect tx-mode

no mac address-table learning [secure]

no mtu

no mvr immediate-leave

no mvr name <mvr_name> type

no mvr vlan <v_vlan_list> type

no platform phy mode

no port-security

no port-security maximum

no port-security sticky

no port-security violation

no priority-flowcontrol prio <prio>

no pvlan <pvlan_list>

no pvlan isolation

no qos cos

no qos dei

no qos dpl

no qos dscp-classify

no qos dscp-remark

no qos dscp-translate

no qos map cos-tag cos <cos> dpl <dpl>

no qos map tag-cos pcp <pcp> dei <dei>

no qos pcp

no qos policer

no qos queue-policer queue <queue>

no qos queue-shaper queue <queue>

no qos shaper

no qos storm { unicast | broadcast | unknown }
no qos tag-remark
no qos trust dscp
no qos trust tag
no qos wred-group
no qos wrr
no rmon collection history <id>
no rmon collection stats <id>
no sflow [<sampler_idx_list>]
no sflow counter-poll-interval [<sampler_idx_list>]
no sflow max-sampling-size [sampler <sampler_idx_list>]
no sflow sampler-type [sampler <sampler_idx_list>]
no shutdown
no spanning-tree
no spanning-tree auto-edge
no spanning-tree bpdu-guard
no spanning-tree edge
no spanning-tree link-type
no spanning-tree mst <instance> cost
no spanning-tree mst <instance> port-priority
no spanning-tree restricted-role
no spanning-tree restricted-tcn
no speed
no switchport access vlan
no switchport forbidden vlan
no switchport hybrid acceptable-frame-type
no switchport hybrid allowed vlan
no switchport hybrid egress-tag
no switchport hybrid ingress-filtering
no switchport hybrid native vlan
no switchport hybrid port-type
no switchport mode
no switchport trunk allowed vlan
no switchport trunk native vlan
no switchport trunk vlan tag native
no switchport vlan ip-subnet <ipv4>

no switchport vlan mac <mac_addr> [vlan <vlan_id>]

no switchport vlan protocol group <grp_id> [vlan <vlan_id>]

no switchport voice vlan discovery-protocol

no switchport voice vlan mode

no switchport voice vlan security

no udld port

platform phy mode { wan | 1g }

port-security

port-security maximum { <v_1_to_1024> }

port-security sticky

port-security sticky <v_mac_addr> vlan <v_vlan_id>

port-security violation { protect | trap | trap-shutdown | shutdown }

priority-flowcontrol prio <prio>

pvlan <pvlan_list>

pvlan isolation

qos cos <cos>

qos dei <dei>

qos dpl <dpl>

qos dscp-classify { zero | selected | any }

qos dscp-remark { rewrite | remap | remap-dp }

qos dscp-translate

qos map cos-tag cos <cos> dpl <dpl> pcp <pcp> dei <dei>

qos map tag-cos pcp <pcp> dei <dei> cos <cos> dpl <dpl>

qos pcp <pcp>

qos policer <rate> [kbps | mbps | fps | kfps] [flowcontrol]

qos queue-policer queue <queue> <rate> [kbps | mbps]

qos queue-shaper queue <queue> <rate> [kbps | mbps] [excess] [rate-type { line | data }]

qos shaper <rate> [kbps | mbps] [rate-type { line | data }]

qos storm { unicast | broadcast | unknown } <rate> [fps | kfps | kbps | mbps]

qos tag-remark { pcp <pcp> dei <dei> | mapped }

qos trust dscp

qos trust tag

qos wred-group <wred_group>

qos wrr <w0> <w1> [<w2> [<w3> [<w4> [<w5> [<w6> [<w7>]]]]]]

rmon collection history <id> [buckets <buckets>] [interval <interval>]

rmon collection stats <id>

sflow [<sampler_idx_list>]
sflow counter-poll-interval [sampler <sampler_idx_list>] [<poll_interval>]
sflow max-sampling-size [sampler <sampler_idx_list>] [<max_sampling_size>]
sflow sampler-type [sampler <sampler_idx_list>] { rx | tx | all }
sflow sampling-rate [sampler <sampler_idx_list>] [<sampling_rate>]
shutdown
spanning-tree
spanning-tree auto-edge
spanning-tree bpdu-guard
spanning-tree edge
spanning-tree link-type { point-to-point | shared | auto }
spanning-tree mst <instance> cost { <cost> | auto }
spanning-tree mst <instance> port-priority <prio>
spanning-tree restricted-role
spanning-tree restricted-tcn
speed { 10g | 2500 | 1000 | 100 | 10 | 100fx | 100fx-ams | 1000x | 1000x-ams | sfp-auto-ams | auto { [10] [100] [1000] } }
switchport access vlan <pvid>
switchport forbidden vlan { add | remove } <vlan_list>
switchport hybrid acceptable-frame-type { all | tagged | untagged }
switchport hybrid allowed vlan { all | none | [add | remove | except] <vlan_list> }
switchport hybrid egress-tag { none | all [except-native] }
switchport hybrid ingress-filtering
switchport hybrid native vlan <pvid>
switchport hybrid port-type { unaware | c-port | s-port | s-custom-port }
switchport mode { access | trunk | hybrid }
switchport trunk allowed vlan { all | none | [add | remove | except] <vlan_list> }
switchport trunk native vlan <pvid>
switchport trunk vlan tag native
switchport vlan ip-subnet [id <1-128>] <ipv4> vlan <vid>
switchport vlan mac <mac_addr> vlan <vid>
switchport vlan protocol group <grp_id> vlan <vid>
switchport voice vlan discovery-protocol { oui | lldp | both }
switchport voice vlan mode { auto | force | disable }
switchport voice vlan security
udld port [aggressive] [message time-interval <v_interval>]

Interface Config Mode Commands (VLANs)

do	To run exec commands in config mode
end	Go back to EXEC mode
exit	Exit from current mode
help	Description of the interactive help system
ip	Interface Internet Protocol config commands
ipv6	IPv6 configuration commands
no	Negate a command or set its defaults
address	Address configuration
dhcp	Configure DHCP server parameters
igmp	Internet Group Management Protocol
<ipv4_addr>	IP address
dhcp	Enable DHCP
server	Enable DHCP server per VLAN
snooping	Snooping IGMP
compatibility	Interface compatibility
last-member-query-interval	Last Member Query Interval in tenths of seconds
priority	Interface CoS priority
querier	IGMP Querier configuration
query-interval	Query Interval in seconds
query-max-response-time	Query Response Interval in tenths of seconds
robustness-variable	Robustness Variable
unsolicited-report-interval	Unsolicited Report Interval in seconds
auto	Compatible with IGMPv1/IGMPv2/IGMPv3
v1	Forced IGMPv1
v2	Forced IGMPv2
v3	Forced IGMPv3
<0-31744>	0 - 31744 tenths of seconds
<0-7>	CoS priority ranges from 0 to 7
address	IGMP Querier address configuration
election	Act as an IGMP Querier to join Querier-Election
<ipv4_ucast>	A valid IPv4 unicast address
<1-31744>	1 - 31744 seconds
<0-31744>	0 - 31744 tenths of seconds
<1-255>	Packet loss tolerance count from 1 to 255

0 - 31744	seconds
address	Configure the IPv6 address of an interface
mld	Multicasat Listener Discovery
<ipv6_subnet>	IPv6 prefix x:x::y/z
dhcp	Enable DHCPv6 client function

Syntax:

do <command>

end

exit

help

ip address { { <address> <netmask> } | { dhcp [fallback <fallback_address> <fal

lback_netmask> [timeout <fallback_timeout>]] } }

ip dhcp server

ip igmp snooping

ip igmp snooping compatibility { auto | v1 | v2 | v3 }

ip igmp snooping last-member-query-interval <ipmc_lmqi>

ip igmp snooping priority <cos_priority>

ip igmp snooping querier { election | address <v_ipv4_ucast> }

ip igmp snooping query-interval <ipmc_qi>

ip igmp snooping query-max-response-time <ipmc_qri>

ip igmp snooping robustness-variable <ipmc_rv>

ip igmp snooping unsolicited-report-interval <ipmc_uri>

ipv6 address <subnet>

ipv6 address { autoconfig | dhcp [rapid-commit] }

ipv6 mld snooping

ipv6 mld snooping compatibility { auto | v1 | v2 }

ipv6 mld snooping last-member-query-interval <ipmc_lmqi>

ipv6 mld snooping priority <cos_priority>

ipv6 mld snooping querier election

ipv6 mld snooping query-interval <ipmc_qi>

ipv6 mld snooping query-max-response-time <ipmc_qri>

ipv6 mld snooping robustness-variable <ipmc_rv>

ipv6 mld snooping unsolicited-report-interval <ipmc_uri>

no ip address

no ip dhcp server

no ip igmp snooping

no ip igmp snooping compatibility

no ip igmp snooping last-member-query-interval

no ip igmp snooping priority

no ip igmp snooping querier { election | address }

no ip igmp snooping query-interval

no ip igmp snooping query-max-response-time

no ip igmp snooping robustness-variable

no ip igmp snooping unsolicited-report-interval

no ipv6 address [<ipv6_subnet>]

no ipv6 address { autoconfig | dhcp [rapid-commit] }

no ipv6 mld snooping

no ipv6 mld snooping compatibility

no ipv6 mld snooping last-member-query-interval

no ipv6 mld snooping priority

no ipv6 mld snooping querier election

no ipv6 mld snooping query-interval

no ipv6 mld snooping query-max-response-time

no ipv6 mld snooping robustness-variable

no ipv6 mld snooping unsolicited-report-interval

8. Copy Commands

Copy from source to destination.

Note: FW v7.20.0039 added "copy" command merge and replace options.

Syntax

copy { startup-config | running-config | <source_path> } { startup-config | running-config | <destination_path> } [syntax-check] [save-host-key] [ftp-active] [{ merge | replace }]

copy { startup-config | running-config | } { startup-config | running-config | } [syntax-check] [save-host-key] [ftp-active] [{merge | replace}].

Parameters

<url_file>	File in FLASH or on remote server. Syntax: <flash:filename> |<protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]>. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score (_). The maximum length is 255 and a hyphen must not be the first character. The file name content that only contains '.' is not allowed.
running-config	Currently running configuration
startup-config	Startup configuration
|	Output modifiers
merge	merge source file with running-config
replace	replace running-config with source file, default action (default)
syntax-check	Perform syntax check on source configuration
save-host-key	Save the Host key

EXAMPLE 1

```
SM12DP2XA# copy startup-config  running-config syntax-check | include OUT
SM12DP2XA# copy running-config startup-config syntax-check
Building configuration...
% Saving 7696 bytes to flash:startup-config
SM12DP2XA#
```

EXAMPLE 2

```
SM12DP2XA# copy running-config startup-config merge
Building configuration...
% Saving 5085 bytes to flash:startup-config
SM12DP2XA# copy startup-config running-config syntax-check
```

```
SM12DP2XA#
```

EXAMPLE 3

```
SM12DP2XA# copy sftp://root:tn@192.168.1.248/running_192.168.1.203_20110101 running-config save-
host-key replace
% Loading /running_192.168.1.203_20110101 from SFTP server 192.168.1.248
SM12DP2XA#
```

Messages: *% Error loading remote file: Connection timed out (9)*

9. Delete Commands

Delete one file in flash: file system.

Syntax

delete <path>

Parameters

<url_file>	File in FLASH. Syntax: <flash:filename>. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), underscore (_). The maximum length is 57 and hyphen must not be first character. A file name content that only contains '.' is not allowed.

EXAMPLE

```
SM12DP2XA# delete flash:test.txt
% Delete of test.txt failed: No such entity.
SM12DP2XA#
```

10. DIR Commands

Directory of all files in flash: file system.

Syntax

Dir [| begin | exclude | include <LINE>]

Parameters

|	Output modifiers
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match
<LINE>	String to match output lines

EXAMPLE

```
SM12DP2XA# dir
Directory of flash:
    r- 2010-12-31 23:59:59     716 default-config
    rw 2011-01-02 19:58:35    1196 startup-config
2 files, 1912 bytes total.
SM12DP2XA# dir
Directory of flash:
    r- 2010-12-31 23:59:59     716 default-config
    rw 2011-01-01 02:23:30    7696 startup-config
    rw 2011-01-01 00:06:22     716 upload 5-7-18
3 files, 9128 bytes total.
SM12DP2XA#
```

11. Disable Commands

Turn off privileged commands.

Syntax

disable <0-15>

disable [<new_priv>]

Parameters

<0-15> Privilege level

<cr>

EXAMPLE

```
SM12DP2XA# disable ?
    <0-15>
    <cr>
SM12DP2XA# disable 10
SM12DP2XA#
```

12. Do Commands

Run Exec mode commands in Config mode or Interface Config mode..

Syntax

Do <LINE>{[LINE]}

Parameters

<line> Exec Command

EXAMPLE 1

```
SM12DP2XA(config)# do show version brief
Version      : SM12DP2XA (standalone) v7.20.0208
Build Date   : 2024-08-14T17:56:47+08:00
SM12DP2XA(config)#
```

EXAMPLE 2

```
SM12DP2XA(config-if)# do show clock
System Time     : 2024-05-16T09:33:04+00:00


SM12DP2XA(config-if)#
```

13. Dot1X Commands

Configure IEEE Standard for port-based Network Access Control.

Syntax

dot1x authentication timer inactivity <v_10_to_100000>

dot1x authentication timer re-authenticate <v_1_to_3600>

dot1x feature { [guest-vlan] [radius-qos] [radius-vlan] }*1

dot1x guest-vlan <value>

dot1x guest-vlan supplicant

dot1x max-reauth-req <value>

dot1x re-authentication

dot1x system-auth-control

dot1x timeout quiet-period <v_10_to_1000000>

dot1x timeout tx-period <v_1_to_65535>

Parameters

authentication	Authentication
feature	Globally enables/disables a dot1x feature functionality
guest-vlan	Guest VLAN
max-reauth-req	The number of times a Request Identity EAPoL frame is sent without response before considering entering the Guest VLAN
re-authentication	Set Re-authentication state
system-auth-control	Set the global NAS state
timeout	timeout
timer	timer
inactivity	Time in seconds between check for activity on successfully authenticated MAC addresses.
re-authenticate	The period between re-authentication attempts in seconds
<10-1000000>	seconds of inactivity
radius-qos	Globally enables/disables state of RADIUS-assigned QoS.
radius-vlan	Globally enables/disables state of RADIUS-assigned VLAN.
<1-4095>	Guest VLAN ID used when entering the Guest VLAN.
supplicant	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.
<1-255>	number of times max-reauth-req
quiet-period	Time in seconds before a MAC-address that failed authentication gets a new authentication chance.
tx-period	the time between EAPoL retransmissions.
<10-1000000>	seconds timeout quiet-period
<1-65535>	seconds timeout tx-period

EXAMPLE

```
SM12DP2XA(config)# dot1x authentication timer inactivity 50000
SM12DP2XA(config)# dot1x feature guest-vlan radius-vlan
SM12DP2XA(config)# dot1x feature radius-vlan
SM12DP2XA(config)# dot1x guest-vlan 1
SM12DP2XA(config)# dot1x max-reauth-req 90
SM12DP2XA(config)# dot1x guest-vlan supplicant
SM12DP2XA(config)# dot1x re-authentication
SM12DP2XA(config)# dot1x timeout tx-period 9000
SM12DP2XA(config)# dot1x timeout quiet-period 100000
SM12DP2XA(config)#
```

14. Enable Commands

Modify enable password parameters.

Syntax

enable [<new_priv>]

enable password [level <priv>] <password>

enable secret { 0 | 5 } [level <priv>] <password>

Parameters

<0-15>	Choose privileged level
password	Assign the privileged level clear password
secret	Assign the privileged level secret
enable	Modify enable password parameters
<word32>	The UNENCRYPTED (clear-text) password
level	Set exec level password
<1-15>	Level number
0	Specifies an UNENCRYPTED password will follow
5	Specifies an ENCRYPTED secret will follow
<word32>	Password

EXAMPLE 1: In Exec mode:

```
SM12DP2XA# enable 10
SM12DP2XA# enable 14
% No password set
SM12DP2XA# enable 9
SM12DP2XA#
```

EXAMPLE 2: In Config mode:

```
SM12DP2XA(config)# enable password admin
SM12DP2XA(config)# enable password level 15 admin
SM12DP2XA(config)# enable secret 0 admin
SM12DP2XA(config)# enable secret 0 level 15 admin
SM12DP2XA(config)# enable secret 5 adminadmin123!@#
SM12DP2XA(config)# enable secret 5 level 15 adminadmin123!@#
SM12DP2XA(config)#
```

15. Firmware Commands

Firmware upgrade/swap.

Syntax

firmware swap

firmware upgrade <url_file> [save-host-key]

Parameters

swap	Swap between Active and Alternate firmware image.
upgrade	Firmware upgrade
<url_file>	Uniform Resource Locator. It is a specific character string that constitutes a reference to a resource. Syntax: <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name> If the following special characters: space !"#$%&'()*+,/:;<=>?@[\]^`{|}~ need to be contained in the input url string, they should have percent-encoded. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under scor e(_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.
save-host-key	Save the host key.

EXAMPLE

```
SM12DP2XA# firmware swap
Active image is managed.bk, alternate image activation is disabled
SM12DP2XA# firmware upgrade
SM12DP2XA#
SM12DP2XA# firmware upgrade sftp ?
                          ^
% Incomplete word detected at '^' marker.
```

16. IP Commands

IPv4 command to retry the DHCP interface VLAN.

Syntax

ip dhcp retry interface vlan <vlan_id>

Parameters

dhcp	Dhcp commands
retry	Restart the DHCP query process
interface	Interface
vlan	Vlan interface
<vlan_id>	Vlan ID

EXAMPLE

```
SM12DP2XA# ip dhcp retry interface vlan 10
% Failed to restart DHCP client on VLAN = 10.
SM12DP2XA#
```

17. No Commands

Negate a command or set its defaults.

Syntax

no debug interrupt-monitor source <source>
no debug ipv6 nd
no debug misc busydeadlock
no debug trace hunt
no port-security shutdown [interface (<port_type> [<v_port_type_list>])]
no terminal editing
no terminal exec-timeout
no terminal history size
no terminal length
no terminal width

Parameters

debug	Debugging functions
port-security	Port security (MAC limit)
terminal	Set terminal line parameters
interrupt-monitor	Print out of reception of the selected interrupt source.
trace hunt	
ipv6	IPv6 configuration commands
misc	Miscellaneous commands
shutdown	Reopen one or more ports whose limit is exceeded and shut down.
source	The selected interrupt source.
<uint>	The possible values are enum vtss_interrupt_source_t values found in file board/interrupt_api.h
nd	IPv6 Neighbor Discovery debugging
busydeadlock	display message
interface	interface type
*	All switches or All ports
GigabitEthernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14
<port_type_list>	Port list in 1/1-2
editing	Enable command line editing
exec-timeout	Set the EXEC timeout
history	Control the command history function
length	Set number of lines on a screen
width	Set width of the display terminal
size	Set history buffer size
<uint>	The possible values are enum vtss_interrupt_source_t values found in file board/interrupt_api.h

EXAMPLE

```
SM12DP2XA# no port-security shutdown
SM12DP2XA# no debug ipv6 nd
SM12DP2XA#
```

18. Ping Commands

Send ICMP echo messages.

Syntax

ping ip { <v_ip_addr> | <v_ip_name> } [repeat <count>] [size <size>] [interval <seconds>]

ping ipv6 { <v_ipv6_addr> | <v_ipv6_name> } [repeat <count>] [size <size>] [interval <seconds>] [interface vlan <v_vlan_id>]

Parameters

ip	IP (ICMP) echo
<word1-255>	ICMP destination address
repeat	Specify repeat count
<1-60>	1-60; Default is 5
size	Specify datagram size
interval	Specify repeat interval
ipv6	IPv6 (ICMPv6) echo
<ipv6_addr>	ICMPv6 destination address
<2-1452>	2-1452; Default is 56 (excluding MAC, IP and ICMP headers)
<0-30>	0-30; Default is 0
interface	Select an interface to configure
vlan	VLAN Interface
<vlan_id>	VLAN identifier(s): VID

EXAMPLE

```
SM12DP2XA# ping ip 192.168.1.77 interval 1 repeat 3 size 30
PING server 192.168.1.77, 30 bytes of data.
38 bytes from 192.168.1.77: icmp_seq=0, time<10ms
38 bytes from 192.168.1.77: icmp_seq=1, time<10ms
38 bytes from 192.168.1.77: icmp_seq=2, time<10ms
Sent 3 packets, received 3 OK, 0 bad
SM12DP2XA#
```

19. Reload Commands

Reload system.

Syntax

reload { { { warm } [sid <usid>] } | { defaults [keep-ip] } }

Parameters

warm	Reload warm (CPU restart only).
defaults	Reload defaults without rebooting.
keep-ip	Attepmt to keep VLAN1 IP setup.

EXAMPLE

```
SM12DP2XA# reload ?
    cold        Reload cold.
    defaults    Reload defaults without rebooting.
SM12DP2XA# reload defaults keep-ip
% Reloading defaults, attempting to keep IP address. Please stand by.
SM12DP2XA#
```

20. Send Commands

Send a message to other tty lines.

Syntax

send { * | <session_list> | console 0 | vty <vty_list> } <message>

Parameters

*	All tty lines
<0~16>	Send a message to multiple lines
console	Primary terminal line
0	Send a message to a specific line
vty	Virtual terminal
<0~15>	Send a message to multiple lines
<LINE>	Message to be sent to lines, in 128 characters

EXAMPLE

```
SM12DP2XA# send * Yes I do
Enter TEXT message.  End with the character 'Y'.
y
SM12DP2XA# send * are you there
Enter TEXT message.  End with the character 'a'.
are you there?a

----------------------------------------
*** Message from line 1:
re you there

----------------------------------------
SM12DP2XA#
```

21. Show Commands

Show running system information.

Command	Function
aaa	Authentication, Authorization and Accounting methods
access	Access management
access-list	Access list
aggregation	Aggregation port configuration
broadcast-storm-protection	Broadcast Storm Protection
clock	Configure time-of-day clock
command-history-log	Command Histry List
dot1x	IEEE Standard for port-based Network Access Control
event	Show trap event configuration
format	Display parameter formats in use.
history	Display the session command history
interface	Interface status and configuration
ip	Internet Protocol
ipmc	IPv4/IPv6 multicast configuration
ipv6	IPv6 configuration commands
lacp	LACP configuration/status
line	TTY line information
lldp	Display LLDP neighbors information.
logging	System logging message
loop-protect	Loop protection configuration
mac	Mac Address Table information
map-api-key	show Google Maps API key configuration
monitor	Monitoring different system events
mvr	Multicast VLAN Registration configuration
ntp	Configure NTP
platform	Platform configuration
port-security	Port Security status - Port Security is a module with no direct configuration.
privilege	Display command privilege
process	process
pvlan	PVLAN configuration
qos	Quality of Service
radius-server	RADIUS configuration
rapid-ring	Display Rapid Ring configurations
rmon	RMON statistics
running-config	Show running system information
sflow	Statistics flow.
smtp	Show email information
snmp	Display SNMP configurations
spanning-tree	STP Bridge
switchport	Display switching mode characteristics
system	Show system parameters
tacacs-server	TACACS+ configuration
terminal	Display terminal configuration parameters
udld	Unidirectional Link Detection(UDLD) configurations, statistics and status
upnp	Display UPnP configuration
user-privilege	Users privilege configuration
users	Display information about terminal lines
version	System hardware and software status
vlan	VLAN status
voice	Voice appliance attributes
web	Web

aaa

Show Login methods.

Syntax

show aaa [| {begin | exclude | include } <LINE>]

Parameters

|	Output modifiers
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match
<LINE>	String to match output lines

EXAMPLE

```
SM12DP2XA# show aaa
Authentication :
  console : local, fallback disabled
  telnet  : local, fallback disabled
  ssh     : local, fallback disabled
  http    : local, fallback disabled
  https   : no, fallback disabled
Authorization :
  console : no, commands disabled, fallback disabled
  telnet  : no, commands disabled, fallback disabled
  ssh     : no, commands disabled, fallback disabled
  http    : no, commands disabled, fallback disabled
  https   : no, commands disabled, fallback disabled
Accounting :
  console : no, commands disabled, exec disabled
  telnet  : no, commands disabled, exec disabled
  ssh     : no, commands disabled, exec disabled
  http    : no, commands disabled, exec disabled
  https   : no, commands disabled, exec disabled
SM12DP2XA
```

access

Show Access management.

Syntax

show access management [statistics | <access_id_list>]

Parameters

management	Access management configuration
statistics	Statistics data
< 1~16>	ID of access management entry
|	Output modifiers
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match
<LINE>	String to match output lines

EXAMPLE

```
SM12DP2XA# show access management
Switch access management mode is disabled

W: WEB/HTTPS
S: SNMP
T: TELNET/SSH

Idx VID  Start IP Address               End IP Address                W S T
--- ---  ------------------------------ ------------------------------ - - -
SM12DP2XA# show access management statistics

Access Management Statistics:
-----------------------------
HTTP     Receive:         0    Allow:         0    Discard:         0
HTTPS    Receive:         0    Allow:         0    Discard:         0
SNMP     Receive:         0    Allow:         0    Discard:         0
TELNET   Receive:         0    Allow:         0    Discard:         0
SSH      Receive:         0    Allow:         0    Discard:         0
SM12DP2XA#
```

access-list

Show Access list.

Syntax

show access-list [interface [(<port_type> [<v_port_type_list>])]] [rate-limiter [<rate_limiter_list>]] [ace statistics [<ace_list>]]

show access-list ace-status [static] [link-oam] [loop-protect] [dhcp] [ptp] [upnp] [arp-inspection] [evc] [mep] [ipmc] [ip-source-guard] [ip-mgmt] [tt-loop] [y1564] [dms-client] [dms-server] [dms-ssdp] [dms-onvif] [agv-car] [dms-mdns] [ztp] [rapid-ring] [lacp-on-air] [conflicts] [switch <switch_list>]

Parameters

|	Output modifiers
ace	Access list entry
ace-status	The local ACEs status
interface	Select an interface to configure
rate-limiter	Rate limiter
*	All Switches or All Ports
Gigbitethernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14
<port_type_list>	Port list in 1/1-2
<1~16>	Rate limiter ID
statistics	Traffic statistics
<1~512>	ACE ID
arp-inspection	The ACEs that are configured by ARP Inspection module
conflicts	The ACEs that did not get applied to the hardware due to hardware limitations
dhcp	The ACEs that are configured by DHCP module
dms-client	The ACEs that are configured by DMS module
dms-mdns	The ACEs that are configured by DMS module
dms-onvif	The ACEs that are configured by DMS module
dms-server	The ACEs that are configured by DMS module
dms-ssdp	The ACEs that are configured by DMS module
ip-source-guard	The ACEs that are configured by IP Source Guard module
ipmc	The ACEs that are configured by IPMC module
lacp-on-air	The ACEs that are configured by LACP On Air module
loop-protect	The ACEs that are configured by Loop Protect module
rapid-ring	The ACEs that are configured by RRING module
static	The ACEs that are configured by users manually
upnp	The ACEs that are configured by UPnP module

EXAMPLE 1

```
SM12DP2XA# show access-list ace statistics rate-limiter

Switch access-list ace number: 0

Switch access-list rate limiter ID 1 is 10 pps
Switch access-list rate limiter ID 2 is 10 pps
Switch access-list rate limiter ID 3 is 10 pps
Switch access-list rate limiter ID 4 is 10 pps
Switch access-list rate limiter ID 5 is 10 pps
Switch access-list rate limiter ID 6 is 10 pps
Switch access-list rate limiter ID 7 is 10 pps
```

```
Switch access-list rate limiter ID 8 is 10 pps
Switch access-list rate limiter ID 9 is 10 pps
Switch access-list rate limiter ID 10 is 10 pps
Switch access-list rate limiter ID 11 is 10 pps
Switch access-list rate limiter ID 12 is 10 pps
Switch access-list rate limiter ID 13 is 10 pps
Switch access-list rate limiter ID 14 is 10 pps
Switch access-list rate limiter ID 15 is 10 pps
Switch access-list rate limiter ID 16 is 10 pps
SM12DP2XA#
```

EXAMPLE 2

```
SM12DP2XA# show access-list ace-status arp-inspection conflicts
User
----
S   : static
IPSG: ipSourceGuard
IPMC: ipmc
ARPI: arpInspection
UPnP: upnp
DHCP: dhcp
LOOP: loopProtect
DMSC: DMS CLIENT
DMSS: DMS Server
DMSD: DMS SSDP
DMSO: DMS Onvif
DMSM: DMS mDNS
RING: Rapid Ring
LACP: LACP On Air
Switch 1 access-list ace number: 0
SM12DP2XA#
```

EXAMPLE 3

```
SM12DP2XA# show access-list ace statistics 1 interface 10GigabitEthernet 1/1

Switch access-list ace number: 0


10GigabitEthernet 1/1 :
-----------------------
10GigabitEthernet 1/1 access-list action is permit
10GigabitEthernet 1/1 access-list policy ID is 0
10GigabitEthernet 1/1 access-list rate limiter ID is disabled
10GigabitEthernet 1/1 access-list redirect is disabled
10GigabitEthernet 1/1 access-list mirror is disabled
10GigabitEthernet 1/1 access-list logging is disabled
10GigabitEthernet 1/1 access-list shutdown is disabled
10GigabitEthernet 1/1 access-list port-state is enabled
10GigabitEthernet 1/1 access-list counter is 0
SM12DP2XA#
```

aggregation

Show Aggregation configuration.

Syntax

show aggregation [mode] [| {begin | exclude | include } <LINE>]

Parameters

mode	Traffic distribution mode
|	Output modifiers
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match
<LINE>	String to match output lines

EXAMPLE

```
SM12DP2XA# show aggregation mode
Aggregation Mode:

SMAC  : Enabled
DMAC  : Disabled
IP    : Enabled
Port  : Enabled
SM12DP2XA#
```

bcs protection

Display Broadcast Storm Protection config.

Syntax

show bcs-protection [interface (<port_type> [<v_port_type_list>])]

Parameters

|	Output modifiers
interface	Select an interface to configure
*	All switches or All ports
GigabitEthernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list for all port types
<port_type_list>	Port list in 1/1-14
<port_type_list>	Port list in 1/1-2

EXAMPLE

```
SM12DP2XA# show broadcast-storm-protection ?
   |           Output modifiers
   interface    Select an interface to configure
   <cr>
SM12DP2XA# show broadcast-storm-protection
Port  Mode      Action           PPS      Timer(seconds)  Status
----  --------  ---------------  -------  --------------  ---------
1     Disable   Shutdown         0        300
2     Disable   Shutdown         0        300
3     Disable   Shutdown         0        300
4     Disable   Shutdown         0        300
5     Disable   Shutdown         0        300
6     Disable   Shutdown         0        300
7     Disable   Shutdown         0        300
8     Disable   Shutdown         0        300
9     Disable   Shutdown         0        300
10    Disable   Shutdown         0        300
11    Disable   Shutdown         0        300
12    Disable   Shutdown         0        300
13    Disable   Shutdown         0        300
14    Disable   Shutdown         0        300
15    Disable   Shutdown         0        300
16    Disable   Shutdown         0        300
SM12DP2XA#
```

clock

Show time-of-day clock.

Syntax

show clock [detail]

Parameter

detail Display detailed clock information

EXAMPLE

```
SM12DP2XA# show clock
System Time     : 2011-01-01T15:32:09+00:00

SM12DP2XA# show clock detail
System Time     : 2011-01-01T15:32:15+00:00

Timezone : Timezone Offset : 0 ( 0 minutes)
Timezone Acronym :

Daylight Saving Time Mode : Disabled.
Daylight Saving Time Start Time Settings :
       Week: 1
       Day: 1
       Month: 1
       Date: 1
       Year: 2014
       Hour: 0
       Minute: 0
Daylight Saving Time End Time Settings :
       Week: 1
       Day: 1
       Month: 1
       Date: 1
       Year: 2097
       Hour: 0
       Minute: 0
Daylight Saving Time Offset : 1 (minutes)
SM12DP2XA#
```

command-history-log

Show Command History list.

Syntax

show command-history-log status

Parameters

status Enable/Disable to Save Command Histry to Flash

EXAMPLE

```
SM12DP2XA# show command-history-log status
The status of termal for Command History Feature : Disable
SM12DP2XA#
```

dot1x

Show parameters for IEEE Standard for port-based Network Access Control.

Syntax

show dot1x statistics { eapol | radius | all } [interface (<port_type> [<v_port_type_list>])]

show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief]

Parameters

statistics	Shows statistics for either eapol or radius.
all	Show all dot1x statistics
eapol	Show EAPOL statistics
radius	Show Backend Server statistics
status	Shows dot1x status, such as admin state, port state and last source.
brief	Show status in a brief format
interface	Interface
*	All Switches or All Ports
Gigbitethernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet
<port_type_list>	Port list in 1/1-2

EXAMPLE

```
SM12DP2XA# show dot1x statistics radius interface GigabitEthernet 1/13
                      Rx Access   Rx Other    Rx Auth.    Rx Auth.    Tx          MAC
Interface             Challenges  Requests    Successes   Failures    Responses   Address
--------------------  ----------  ----------  ----------  ----------  ----------  -------
GigabitEthernet 1/13   0          0          0          0          0               -
SM12DP2XA# show dot1x status brief interface GigabitEthernet 1/13
Inf      Admin  Port State  Last Src          Last ID             QOS   VLAN  Guest
--------  -----  ----------  -----------------  -----------------  ----  ----  ------
Gi 1/13   Auth   Auth       -                   -                   -     -     -

SM12DP2XA#
```

event

Show trap event configuration.

Syntax

show event
show event port

EXAMPLE

```
SM12DP2XA# show event port
SM12DP2XA# show event <cr>
Group Name                       Severity Level    Syslog Mode   Trap Mode        SMTP Mode
-------------------------------  ----------------  ------------  -----------------------
AC-Power                         Info              enable        disable          disable
ACL                              Info              enable        disable          disable
ACL-Log                          Info              enable        disable          disable
Access-Mgmt                      Info              enable        disable          disable
Auth-Failed                      Warning           enable        disable          disable
BCS-Protection                   Info              enable        disable          disable
Cold-Start                       Warning           enable        disable          disable
Config-Info                      Info              enable        disable          disable
DC-Power                         Info              enable        disable          disable
DMS                              Info              enable        disable          disable
Dying-Gasp                       Crit              enable        disable          disable
FAN                              Warning           enable        disable          disable
Firmware-Upgrade                 Info              enable        disable          disable
Import-Export                    Info              enable        disable          disable
LACP                             Info              enable        disable          disable
Link-Status                      Warning           enable        disable          disable
Login                            Info              enable        disable          disable
Logout                           Info              enable        disable          disable
Loop-Protect                     Info              enable        disable          disable
Mgmt-IP-Change                   Info              enable        disable          disable
Module-Change                    Warning           enable        disable          disable
NAS                              Info              enable        disable          disable
Password-Change                  Info              enable        disable          disable
Port-Security                    Info              enable        disable          disable
SCP-Fail                         Warning           enable        disable          disable
SCP-Success                      Info              enable        disable          disable
Spanning-Tree                    Info              enable        disable          disable
Temperature                      Warning           enable        disable          disable
Voltage                          Warning           enable        disable          disable
Warm-Start                       Warning           enable        disable          disable
SM12DP2XA#
```

format

Show date/time/port format information.

Syntax

show format

EXAMPLE

```
SM12DP2XA# show format
formatDateTime : disable
dateTime       : yyyy-mm-dd
timeFormat     : 24 hour
formatPortDesc : disable
SM12DP2XA#
```

history

Display the session command history.

Syntax

show history [| {begin | exclude | include } <LINE>]

Parameters

|	Output modifiers
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match
<LINE>	String to match output lines

EXAMPLE

```
SM12DP2XA# show history
  show event port
  show event
  show history
SM12DP2XA#

SM12DP2XA# show history
  platform debug allow
  help
  show event port
  show event
  show event port
  show event port 1/1-2
  show event port
  show history
SM12DP2XA#
```

interface

Display Interface status and configuration.

Syntax

show interface (<port_type> [<in_port_list>]) switchport [access | trunk |hybrid]

show interface (<port_type> [<v_port_type_list>]) CableDiag

show interface (<port_type> [<v_port_type_list>]) capabilities [detail]

show interface (<port_type> [<v_port_type_list>]) description

show interface (<port_type> [<v_port_type_list>]) statistics [{ packets | bytes | errors | discards | filtered | { priority [<priority_v_0_to_7>] } }] [{ up | down }]

show interface (<port_type> [<v_port_type_list>]) status

show interface vlan [<vlist>]

Parameters

<port_type>	* or Gigabitethernet
*	All Switches or All ports
GigabitEthernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
CableDiag	Display the latest cable diagnostic results.
capabilities	Display capabilities.
description	Show port description.
statistics	Display statistics counters.
status	Display status.
switchport	Show interface switchport information
veriphy	Run cable diagnostics and show result.
bytes	Show byte statistics.
discards	Show discard statistics.
down	Show ports which are down
errors	Show error statistics.
filtered	Show filtered statistics.
packets	Show packet statistics.
priority	Queue number
up	Show ports which are up
vlan	VLAN status
<vlan_list>	VLAN list
detail	Display capabilities in detail.
|	Output modifiers
access	Show access ports status
hybrid	Show hybrid ports status
trunk	Show trunk ports status

EXAMPLE 1

```
SM12DP2XA# show interface GigabitEthernet 1/2 capabilities

GigabitEthernet 1/2 Capabilities:
     Tx Central                                Mon1      Mon2         Mon3
Port Wavelength  Bit Rate   Temperature   Vcc   (Bias)   (Tx PWR)     (Rx PWR)
---- ---------- ----------- ----------- ------- ------ ------------ ------------
2       1310   1000 Mbps     44.06 C  3.32 V   8 mA    -6.83 dBm        none

Name/Model:           Transition      TN-SFP-LX1
```

```
Type:                1000BASE_LX
Speed:               100,1000,auto
Duplex:              full,auto
Trunk encap. type:    802.1Q
Trunk mode:          access,hybrid,trunk
Channel:             yes
Broadcast suppression: no
Flowcontrol:          yes
Fast Start:           no
QoS scheduling:       tx-(8q)
CoS rewrite:          yes
ToS rewrite:          yes
UDLD:                no
Inline power:         no
RMirror:             yes
PortSecure:          yes
Dot1x:               yes
SM12DP2XA# show interface vlan
VLAN1
  LINK: 00-c0-f2-49-38-bb Mtu:1500 <UP BROADCAST RUNNING MULTICAST>
  IPv4: 192.168.1.77/24 192.168.1.255
  IPv4: 169.254.130.72/16 169.254.255.255
  IPv6: fe80::2c0:f2ff:fe49:38bb/64 <UP RUNNING>
VLAN4096
  LINK: 00-c0-f2-49-38-bb Mtu:1500 <BROADCAST MULTICAST>
VLAN4097
  LINK: 00-c0-f2-49-38-bb Mtu:1500 <BROADCAST MULTICAST>
SM12DP2XA#
```

EXAMPLE 2

```
SM12DP2XA# show interface * switchport
Name: GigabitEthernet 1/1
Administrative mode: access
Access Mode VLAN: 1
Trunk Native Mode VLAN: 1
Administrative Native VLAN tagging: disabled
Allowed VLANs: 1-4095
Hybrid port configuration
-------------------------
Port Type: C-Port
Acceptable Frame Type: All
Ingress filter: Disabled
Egress tagging: All except-native
Hybrid Native Mode VLAN: 1
Hybrid VLANs Enabled: 1-4095

Name: GigabitEthernet 1/2
Administrative mode: access
Access Mode VLAN: 1
Trunk Native Mode VLAN: 1
Administrative Native VLAN tagging: disabled
Allowed VLANs: 1-4095
Hybrid port configuration
-- more --, next page: Space, continue: g, quit: ^C
```

ip

Display Internet Protocol information.

Syntax

show ip arp

show ip arp inspection [interface (<port_type> [<in_port_type_list>]) | vlan <in_vlan_list>]

show ip arp inspection entry [dhcp-snooping | static] [interface (<port_type> [<in_port_type_list>])]

show ip dhcp detailed statistics { server | client | snooping | relay | normal-forward | combined } [interface (<port_type> [<in_port_list>])]

show ip dhcp excluded-address

show ip dhcp pool [<pool_name>]

show ip dhcp relay [statistics]

show ip dhcp server

show ip dhcp server binding <ip>

show ip dhcp server binding [state { allocated | committed | expired }] [type { automatic | manual | expired }]

show ip dhcp server declined-ip

show ip dhcp server declined-ip <declined_ip>

show ip dhcp server statistics

show ip dhcp snooping [interface (<port_type> [<in_port_list>])]

show ip dhcp snooping table

show ip domain

show ip gateway interface

show ip http

show ip http server secure status

show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

show ip igmp snooping mrouter [detail]

show ip interface brief

show ip name-server

show ip route

show ip source binding [dhcp-snooping | static] [interface (<port_type> [<in_port_type_list>])]

show ip ssh

show ip ssh key

show ip statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

show ip telnet

show ip verify source [interface (<port_type> [<in_port_type_list>])]

Parameters

arp	Address Resolution Protocol
dhcp	Dynamic Host Configuration Protocol
domain	Default domain name
gateway	Gateway address binding interface
http	Hypertext Transfer Protocol
igmp	Internet Group Management Protocol
interface	IP interface status and configuration
link-local	Link-local
name-server	Domain Name System
route	Display the current IP routing table
source	source command
ssh	Secure Shell

statistics	Traffic statistics
telnet	TELNET
verify	verify command
inspection	ARP inspection
interface	arp inspection entry interface config
<port_type>	Gigabitethernet
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet
vlan	VLAN configuration
<vlan_list>	Select a VLAN id to configure
entry	arp inspection entries
dhcp-snooping	learn from dhcp snooping
static	setting from static entries
relay	DHCP relay agent configuration
statistics	Traffic statistics
snooping	DHCP snooping
server	HTTP web server
secure	Secure
status	Status
igmp	Internet Group Management Protocol
snooping	Snooping IGMP
vlan	Search by VLAN
<vlan_list>	VLAN identifier(s): VID
group-database	Multicast group database from IGMP
sfm-information	Including source filter multicast information from IGMP
detail	Detail running information/statistics of IGMP snooping
mrouter	Multicast router port status in IGMP
detail	Detail running information/statistics of IGMP snooping
brief	Brief IP interface status
binding	ip source binding
dhcp-snooping	learn from dhcp snooping
system	IPv4 system traffic
icmp	IPv4 ICMP traffic
icmp-msg	IPv4 ICMP traffic for designated message type
<0~255>	ICMP message type ranges from 0 to 255

EXAMPLE 1

```
SM12DP2XA# show ip interface brief
Vlan Address             Method   Status
---- -------------------- -------- ------
   1 192.168.1.77/24      Manual   UP
SM12DP2XA# show ip statistics

IPv4 statistics:

  Rcvd:  645972 total in 65095614 bytes
         324818 local destination, 0 forwarding
         0 header error, 1684 address error, 0 unknown protocol
         0 no route, 0 truncated, 1798 discarded
  Sent:  488388 total in 57968178 bytes
         323006 generated, 0 forwarded
         0 no route, 0 discarded
  Frags: 0 reassemble (0 reassembled, 0 couldn't reassemble)
         0 fragment (0 fragmented, 0 couldn't fragment)
```

```
        0 fragment created
  Mcast: 155772 received in 7649660 bytes
        153974 sent in 7463602 bytes
  Bcast: 155658 received, 153974 sent

IP interface statistics:

  IPv4 Statistics on Interface VLAN: 1
  Rcvd:  157604 total in 7907241 bytes
        79718 local destination, 0 forwarding
-- more --, next page: Space, continue: g, quit: ^C

# show ip link-local interface ?
    |      Output modifiers
    <cr>
SM12DP2XA# show ip link-local interface
Link-Local Address binding interface: 1
SM12DP2XA# show ip link-local interface
Link-Local Address binding interface: 100
SM12DP2XA#
```

EXAMPLE 2

```
SM12DP2XA# show ip dhcp server
DHCP server is globally disabled.
  All VLANs are disabled.
  DHCP server per port is disabled.

SM12DP2XA# show ip domain
Current domain name is not configured.

SM12DP2XA# show ip gateway interface
Gateway Address binding interface: 1

SM12DP2XA(config)# ip gateway interface 100
SM12DP2XA(config)# do show ip gateway interface
Gateway Address binding interface: 100

SM12DP2XA# show ip ssh
Switch SSH is enabled
Switch SSH port is 22
Switch scp is disabled

SM12DP2XA# show ip ssh key
ECDSA:
Public key portion is:
 521 ecdsa-sha2-nistp521 AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBAH
dzCVJuGqawCAFsr7XBQPABAgvTsLRGKGkU1H7udELGWrj5ApJ4NB7fEjhDnDlK0FjiFSMoEggijuSm49
aIRJMRwEKOzF7IJCXxXwZXxUQP6h1HlcvLGPO9cpgx/0tlF3ylWW4u67IHoqG5WUmRfOc95rPIBAXK5E
gWyLrtu4CiZX0yg==
ECDSA: md5 5c:ef:09:91:95:64:8c:82:69:81:76:16:03:b6:aa:db

SM12DP2XA# show ip telnet
Switch Telnet server is enabled
Switch TELNET server port is 23

SM12DP2XA# show ip igmp snooping
IGMP Snooping is disabled to stop snooping IGMP control plane.
SM12DP2XA# show ip igmp snooping
IGMP Snooping is enabled to start snooping IGMP control plane.
Switch-1 IGMP Interface Status
IGMP snooping VLAN 10 interface is enabled.
Querier status is ACTIVE
RX IGMP Query:0 V1Join:0 V2Join:0 V3Join:0 V2Leave:0
```

```
TX IGMP Query:0 / (Source) Specific Query:0
Compatibility:IGMP-Auto / Querier Version:Default / Host Version:Default
SM12DP2XA#
```

ipmc

Show IPv4/IPv6 multicast configuration.

Syntax

show ipmc profile [<profile_name>] [detail]
show ipmc range [<entry_name>]

Parameters

profile	IPMC profile configuration
range	A range of IPv4/IPv6 multicast addresses for the profile
< word16>	Profile name in 16 char's
detail	Detail information of a profile
< word16>	Range entry name in 16 char's
|	Output modifiers
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match
<LINE>	String to match output lines

EXAMPLE

```
SM12DP2XA# show ipmc profile detail

IPMC Profile is currently disabled, please enable profile to start filtering.
SM12DP2XA#

SM12DP2XA# show ipmc profile

IPMC Profile is now enabled to start filtering.

Profile: Prof1 (In VER-INI Mode)
Description:

Profile: Profile1 (In VER-INI Mode)
Description: IPMC filtering profile 2-11-21

Profile: test (In VER-INI Mode)
Description:

SM12DP2XA# show ipmc range

Range Name   : Range1
Start Address: 224.99.99.99
End Address  : 224.99.99.99
SM12DP2XA#
```

ipv6

Show IPv6 configuration commands.

Syntax

show ipv6 dhcp-client [interface vlan <v_vlan_list>]

show ipv6 interface [vlan <v_vlan_list> { brief | statistics }]

show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

show ipv6 mld snooping mrouter [detail]

show ipv6 neighbor [interface vlan <v_vlan_list>]

show ipv6 route [interface vlan <v_vlan_list>]

show ipv6 statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

Parameters

interface	Select an interface to configure
vlan	VLAN of IPv6 interface
<vlan_list>	IPv6 interface VLAN list
brief	Brief summary of IPv6 status and configuration
statistics	Traffic statistics
mld	Multicasat Listener Discovery
snooping	Snooping MLD
vlan	Search by VLAN
<vlan_list>	VLAN identifier(s): VID
group-database	Multicast group database from MLD
interface	Search by port
<port_type>	* or Gigabitethernet
*	All Switches or All ports
Gigabitethernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet
sfm-information	Including source filter multicast information from MLD
detail	Detail running information/statistics of MLD snooping
mrouter	Multicast router port status in MLD
neighbor	IPv6 neighbors
route	IPv6 routes
statistics	Traffic statistics
system	IPv6 system traffic
icmp	IPv6 ICMP traffic
icmp-msg	IPv6 ICMP traffic for designated message type
<Type : 0~255>	ICMP message type ranges from 0 to 255

EXAMPLE 1

```
SM12DP2XA# show ipv6 interface vlan 1 brief
IPv6 Vlan1 interface is up.
  Internet address is fe80::2c0:f2ff:fe49:38dd
  Static address is not set
SM12DP2XA# show ipv6 interface
IPv6 Vlan1 interface is up.
  Internet address is fe80::2c0:f2ff:fe49:38dd
  Static address is not set
```

```
  IP stack index (IFID) is 5
  Routing is disabled on this interface
  MTU is 1500 bytes
  IPv6 Statistics on Interface VLAN: 1
  Rcvd:  0 total in 0 byte
         0 local destination, 0 forwarding
         0 header error, 0 address error, 0 unknown protocol
         0 no route, 0 truncated, 0 discarded
  Sent:  10 total in 656 bytes
         10 generated, 0 forwarded
         0 discarded
  Frags: 0 reassemble (0 reassembled, 0 couldn't reassemble)
         0 fragment (0 fragmented, 0 couldn't fragment)
         0 fragment created
  Mcast: 0 received in 0 byte
         10 sent in 656 bytes
  Bcast: 0 received, 0 sent
SM12DP2XA# show ipv6 mld snooping
MLD Snooping is disabled to stop snooping MLD control plane.
SM12DP2XA# show ipv6 neighbor
fe80::2c0:f2ff:fe49:38dd via VLAN1: 00-c0-f2-49-38-dd Permanent/REACHABLE
SM12DP2XA#
```

EXAMPLE 2

```
SM12DP2XA# show ipv6 statistics system

IPv6 statistics:

  Rcvd:  0 total in 0 byte
         0 local destination, 0 forwarding
         0 header error, 0 address error, 0 unknown protocol
         0 no route, 0 truncated, 0 discarded
  Sent:  10 total in 656 bytes
         14 generated, 0 forwarded
         0 no route, 0 discarded
  Frags: 0 reassemble (0 reassembled, 0 couldn't reassemble)
         0 fragment (0 fragmented, 0 couldn't fragment)
         0 fragment created
  Mcast: 0 received in 0 byte
         10 sent in 656 bytes
  Bcast: 0 received, 0 sent
SM12DP2XA#
```

lacp

Display LACP configuration/status.

Syntax

show lacp on-air
show lacp { internal | statistics | system-id | neighbor }

Parameters

internal	Internal LACP configuration
neighbor	Neighbor LACP status
on-air	LACP On Air configuration
statistics	Internal LACP statistics
system-id	LACP system id
|	Output modifiers
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match
<LINE>	String to match output lines

EXAMPLE

```
SM12DP2XA# show lacp system-id
System Priority: 32768
SM12DP2XA# show lacp internal
Port                Mode      Key   Role    Timeout  Priority
------------------  --------  ----  ------  -------  --------
Gi 1/1              disabled   Auto  Active  Fast     32768
Gi 1/2              disabled   Auto  Active  Fast     32768
Gi 1/3              disabled   Auto  Active  Fast     32768
Gi 1/4              disabled   Auto  Active  Fast     32768
Gi 1/5              disabled   Auto  Active  Fast     32768
Gi 1/6              disabled   Auto  Active  Fast     32768
Gi 1/7              disabled   Auto  Active  Fast     32768
Gi 1/8              disabled   Auto  Active  Fast     32768
Gi 1/9              disabled   Auto  Active  Fast     32768
Gi 1/10             disabled   Auto  Active  Fast     32768
Gi 1/11             disabled   Auto  Active  Fast     32768
Gi 1/12             disabled   Auto  Active  Fast     32768
Gi 1/13             disabled   Auto  Active  Fast     32768
Gi 1/14             disabled   Auto  Active  Fast     32768
10G 1/1             disabled   Auto  Active  Fast     32768
10G 1/2             disabled   Auto  Active  Fast     32768
SM12DP2XA#
```

line

Show TTY line information.

Syntax

show line [alive] [| {begin | exclude | include } <LINE>]

Parameters

alive	Display information about alive lines
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match
<LINE>	String to match output lines

EXAMPLE

```
SM12DP2XA# show line alive
Line is vty 0.
    * You are at this line now.
    Alive from Telnet.
    Default privileged level is 2.
    Command line editing is enabled
    Display EXEC banner is enabled.
    Display Day banner is enabled.
    Terminal width is 80.
            length is 24.
            history size is 32.
            exec-timeout is 10 min 0 second.

    Current session privilege is 15.
    Elapsed time is 0 day 0 hour 49 min 45 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

SM12DP2XA# show line
Line is con 0.
    Not alive.
    Default privileged level is 2.
    Command line editing is disabled
    Display EXEC banner is enabled.
    Display Day banner is enabled.
    Terminal width is 80.
            length is 24.
            history size is 32.
            exec-timeout is 10 min 0 second.

    Current session privilege is 0.
    Elapsed time is 0 day 0 hour 0 min 0 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

Line is vty 0.
```

```
    * You are at this line now.
    Alive from Telnet.
    Default privileged level is 2.
    Command line editing is disabled
    Display EXEC banner is enabled.
    Display Day banner is enabled.
    Terminal width is 80.
            length is 24.
            history size is 14.
            exec-timeout is 1440 min 0 second.

    Current session privilege is 15.
    Elapsed time is 0 day 0 hour 38 min 7 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

Line is vty 1.
    Not alive.
    Default privileged level is 2.
    Command line editing is disabled
    Display EXEC banner is enabled.
    Display Day banner is enabled.
    Terminal width is 80.
            length is 24.
            history size is 32.
            exec-timeout is 10 min 0 second.

    Current session privilege is 0.
    Elapsed time is 0 day 0 hour 0 min 0 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.
-- more --, next page: Space, continue: g, quit: ^C
```

lldp

Display LLDP neighbors information..

Syntax

show lldp [interface (<port_type> [<v_port_type_list>])]
show lldp med media-vlan-policy [<v_0_to_31>]
show lldp med remote-device [interface (<port_type> [<port_list>])]
show lldp neighbors [interface (<port_type> [<v_port_type_list>])]
show lldp statistics [interface (<port_type> [<v_port_type_list>])]

Parameters

med	Display LLDP-MED neighbors information.
neighbors	Display LLDP neighbors information.
statistics	Display LLDP statistics information.
media-vlan-policy	Display media vlan policies.
remote-device	Display remote device LLDP-MED neighbors information.
<0~31>	List of policies.
Interface	Interface to display.
<port_type >	GigabitEthernet
*	All Switches or All ports
Gigabitethernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-2
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet

EXAMPLE

```
SM12DP2XA# show lldp
LLDP Configuration
------------------
TX Interval : 30
TX Hold : 4
TX Delay : 2
TX Reinit : 2
SM12DP2XA#
SM12DP2XA# show lldp statistics
LLDP global counters
Neighbor entries was last changed at 2010-12-31T23:59:59+00:00  (60254 secs. ago).
Total Neighbors Entries Added    0.
Total Neighbors Entries Deleted  0.
Total Neighbors Entries Dropped  0.
Total Neighbors Entries Aged Out 0.

LLDP local counters
                     Rx       Tx       Rx       Rx        Rx TLV   Rx TLV   Rx TLV
Interface             Frames   Frames   Errors   Discards  Errors   Unknown  Organiz.  Aged
---------             ------   ------   ------   --------  ------   -------  --------  ----
GigabitEthernet 1/1    0        0        0        0         0        0        0         0
GigabitEthernet 1/2    0        0        0        0         0        0        0         0
GigabitEthernet 1/3    0        0        0        0         0        0        0         0
-- more --, next page: Space, continue: g, quit: ^C
```

logging

Display Syslog information.

Syntax

show logging <log_id> [switch <switch_list>]
show logging [info] [warning] [error] [emerg] [alert] [crit] [notice] [debug] [switch <switch_list>] [reverse]
show logging flash [category { debug | system | application }] [level { informational | notice | warning | error }]

Parameters

<1-4294967295>	Logging ID
|	Output modifiers
alert	Severity 1: Action must be taken immediately
crit	Severity 2: Critical conditions
debug	Severity 7: Debug-level messages
emerg	Severity 0: System is unusable
error	Severity 3: Error conditions
flash	Logging message on Flash
info	Severity 6: Informational messages
notice	Severity 5: Normal but significant condition
warning	Severity 4: Warning conditions
category	Category of logging message
level	Severity level
application	Application category
debug	Debug category
system	System category
informational	Severity 6: Informational messages
exclude	Exclude lines that match
include	Include lines that match
switch	Switch
<switch_list>	Switch ID list in 1

EXAMPLE 1:

```
SM12DP2XA# show logging
Switch logging host mode is disabled
Switch logging host address is null
Switch logging host port is 514
Number of entries on Switch 1:
Emerg       : 0
Alert       : 0
Crit        : 0
Error       : 0
Warning     : 6
Notice      : 2
Info        : 21
Debug       : 0
All         : 29

ID    Level   Time                      Message                                    iPush Status
----  ------  ------------------------  -----------------------------------------  ------------
   1  Notice  2011-01-01T00:00:13+00:00  LINK-UPDOWN: Interface Vlan 1, changeds
```

```
   2  Warning 2011-01-01T00:00:13+00:00  Link down on port 14
   3  Info    2011-01-01T00:00:14+00:00  Password of user 'admin' was changed
   4  Warning 2011-01-01T00:00:14+00:00  Link up on port 14
   5  Warning 2011-01-01T00:00:14+00:00  SFP module inserted on port 15
   6  Warning 2011-01-01T00:00:14+00:00  SFP module inserted on port 16
   7  Info    2011-01-01T00:00:14+00:00  topologyChange
   8  Warning 2011-01-01T00:00:14+00:00  Switch just made a cold boot
   9  Info    2011-01-01T00:00:14+00:00  topologyChange
-- more --, next page: Space, continue: g, quit: ^C
```

EXAMPLE 2:

```
SM12DP2XA# show logging flash category application level warning
Category    | Level   | Time                      | Message
-------------------------------------------------------------------------------
Application | Warning     | 2011-01-01T03:16:39+00:00 | Bad password attempt for user ''  through
TELNET from 192.168.1.99:50199 and authenticated by unknown method
Application | Warning     | 2011-01-01T00:00:14+00:00 | SFP module inserted on port 3 Connector Type:
SFP or SFP Plus - LC Fiber Type    : Single Mode (SM) Tx Wavelength : 1310 Baud Rate     : 1000 Mbps
Vendor OUI    : 00-c0-f2 Vendor Name    : Transition      Vendor PN     : TN-SFP-LX1      Vendor
Rev    : 0000 Vendor SN     : 9004716         Date Code     : 080502
Application | Warning     | 2011-01-01T00:00:14+00:00 | Switch just made a warm boot
Application | Warning     | 2011-01-01T00:00:15+00:00 | SFP module inserted on port 1 Connector Type:
SFP or SFP Plus - LC Fiber Type    : Reserved Tx Wavelength : 850 Baud Rate     : 10 Gbps Vendor
OUI    : 00-c0-f2 Vendor Name   : Transition      Vendor PN     : TN-10GSFP-SR     Vendor Rev    : 0001
Vendor SN     : 8801095         Date Code     : 120731
-- more --, next page: Space, continue: g, quit: ^C

SM12DP2XA# show logging flash level notice
Category    | Level     | Time                      | Message
-------------------------------------------------------------------------------
Application | Notice    | 2011-01-01T03:42:38+00:00 | LINK-UPDOWN: Interface Vlan 1, changed state to
up.
Application | Notice    | 2011-01-01T19:56:09+00:00 | LINK-UPDOWN: Interface Vlan 1, changed state to
down.
Application | Notice    | 2011-01-01T19:56:11+00:00 | LINK-UPDOWN: Interface Vlan 1, changed state to
up.
Application | Notice    | 2011-01-01T19:57:19+00:00 | LINK-UPDOWN: Interface Vlan 1, changed state to
down.
Application | Notice    | 2011-01-01T19:57:23+00:00 | LINK-UPDOWN: Interface Vlan 1, changed state to
up.
Application | Notice    | 2011-01-01T20:21:08+00:00 | LINK-UPDOWN: Interface Vlan 1, changed state to
up.
SM12DP2XA#
```

EXAMPLE 3:

```
SM12DP2XA# show logging 2 switch 1
Switch : 1
ID     : 2
Level  : Warning
Time   : 2011-01-01T00:00:14+00:00
Message:
SFP module inserted on port 1
Connector Type: SFP or SFP Plus - LC
Fiber Type    : Reserved
Tx Wavelength : 850
Baud Rate     : 10 Gbps
Vendor OUI    : 00-c0-f2
Vendor Name   : Transition
Vendor PN     : TN-10GSFP-SR
Vendor Rev    : 0001
```

```
Vendor SN     : 8801095
Date Code     : 120731
SM12DP2XA# show logging 9 switch 1
Switch : 1
ID     : 9
Level  : Info
Time   : 2011-01-01T00:00:24+00:00
Message: AC Power Up
SM12DP2XA#
```

loop-protect

Loop protection configuration.

Syntax

show loop-protect [interface (<port_type> [<plist>])]

Parameters

interface	Interface status and configuration
<port_type >	GigabitEthernet
*	All Switches or All ports
Gigabitethernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet

EXAMPLE

```
SM12DP2XA# show loop-protect

Loop Protection Configuration
=====================================
Loop Protection   : Disable
Transmission Time : 5 sec
Shutdown Time     : 180 sec

GigabitEthernet 1/1
------------------------------
    Loop protect mode is enabled.
    Action is shutdown.
    Transmit mode is enabled.
    No loop.
    The number of loops is 0.
    Status is down.

GigabitEthernet 1/2
------------------------------
    Loop protect mode is enabled.
    Action is shutdown.
    Transmit mode is enabled.
    No loop.
-- more --, next page: Space, continue: g, quit: ^C
```

mac

Display Mac Address Table information.

Syntax

show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>]) | vlan <v_vlan_id_2>] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])]

Parameters

address-table	Mac Address Table
conf	User added static mac addresses
static	All static mac addresses
aging-time	Aging time
learning	Learn/disable/secure state
count	Total number of mac addresses
interface	Select an interface to configure
<port_type>	* or Gigabitethernet
*	All switches or All ports
Gigabitethernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet
address	MAC address lookup
<mac_addr>	48 bit MAC address: xx:xx:xx:xx:xx:xx
vlan	VLAN lookup
<vlan_id>	VLAN IDs 1-4095
vlan	Addresses in this VLAN
<vlan_id>	VLAN IDs 1-4095
interface	Select an interface to configure
<port_type>	Gigabitethernet

EXAMPLE

```
SM12DP2XA# show mac address-table address 00-c0-f2-49-38-dd
Type    VID  MAC Address       Ports
Static  1    00:c0:f2:49:38:dd   CPU
SM12DP2XA# show mac address-table aging-time
MAC Age Time: 300
SM12DP2XA# show mac address-table learning vlan 1
Vlan 1 learning is enabled
SM12DP2XA# show mac address-table static
Type    VID  MAC Address       Ports
Static  1    00:c0:f2:49:38:bb   CPU
Static  1    33:33:00:00:00:01  GigabitEthernet 1/1-14 10GigabitEthernet 1/1-2 CPU
Static  1    33:33:00:00:00:02  GigabitEthernet 1/1-14 10GigabitEthernet 1/1-2 CPU
Static  1    33:33:ff:49:38:bb  GigabitEthernet 1/1-14 10GigabitEthernet 1/1-2 CPU
Static  1    ff:ff:ff:ff:ff:ff  GigabitEthernet 1/1-14 10GigabitEthernet 1/1-2 CPU

SM12DP2XA#
```

map-api-key

Show Google Maps API key configuration.

Syntax

show map-api-key <cr>

Parameters

| Output modifiers

<cr>

EXAMPLE

```
SM12DP2XA# show map-api-key
Key   :
SM12DP2XA#
```

monitor

Display monitor Mirror session.

Syntax

show monitor [session { <session_number> | all | remote }]

Parameters

<1>	MIRROR session number
all	Show all MIRROR sessions
remote	Show only Remote MIRROR sessions

EXAMPLE

```
SM12DP2XA# show monitor

Session 1
---------
Mode                    : Disabled
Type                    : Mirror
Source VLAN(s)           :
SM12DP2XA#
```

mvr

Display Multicast VLAN Registration configuration.

Syntax

show mvr [vlan <v_vlan_list> | name <mvr_name>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

Parameters

vlan	Search by VLAN
<vlan_list>	MVR multicast VLAN list
name	Search by MVR name
<word16>	MVR multicast VLAN name
group-database	Multicast group database from MVR
interface	Search by port
<port_type>	* or Gigabitethernet
*	All Switches or All ports
Gigabitethernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet
sfm-information	Including source filter multicast information from MVR
detail	Detail information/statistics of MVR group database
|	Output modifiers

EXAMPLE

```
SM12DP2XA# show mvr
MVR is now enabled to start group registration.
SM12DP2XA# show mvr detail
MVR is currently disabled, please enable MVR to start group registration.
SM12DP2XA# show mvr group-database sfm-information
MVR is now enabled to start group registration.
MVR Group Database
Switch-1 MVR Group Count: 0
SM12DP2XA# show mvr name VID11
MVR is now enabled to start group registration.
% Invalid MVR VLAN VID11.
SM12DP2XA#
```

ntp

Show NTP status.

Syntax

show ntp status

Parameters

status status

EXAMPLE

```
SM12DP2XA# show ntp status
NTP Mode : disabled
Idx   Server IP host address (a.b.c.d) or a host name string
---   ----------------------------------------------------
1
2
3
4
5
SM12DP2XA#
SM12DP2XA# show ntp status
NTP Mode : enabled
Automatic: enabled
Idx   Server IP host address (a.b.c.d)
---   ----------------------------------------------------
1

Idx   Server IP host address (a.b.c.d) or a host name string
---   ----------------------------------------------------
1     BobB
2     192.168.1.30
3
4
5
SM12DP2XA#
```

platform

Display Platform specific information.

Syntax

show platform debug
show platform phy [interface (<port_type> [<v_port_type_list>])]
show platform phy id [interface (<port_type> [<v_port_type_list>])]
show platform phy instance
show platform phy mode [interface (<port_type> [<v_port_type_list>])]

Parameters

debug	Debug command setting
phy	PHYs' information
|	Output modifiers
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match
<LINE>	String to match output lines

EXAMPLE

```
SM12DP2XA# show platform debug

Platform debug command function is denied.

SM12DP2XA# show platform phy
Port   API Inst   WAN/LAN/1G Mode      Duplex     Speed      Link
----   ---------  ---------  ----      ------     -----      ----
13     Default    1G         ANEG      -          -          No
14     Default    1G         ANEG      -          -          Yes
SM12DP2XA# show platform phy instance
Next Restart    : Cold
Previous Restart: Cold
Current API Version : 1
Previous API Version: 1
Phy Instance Restart Source:1G
Phy Instance Restart Port:0
Current Phy Start Instance:none
SM12DP2XA# show platform phy mode
% Note: Feature  is only supported on 10G PHYs on port: 1
% Note: Feature  is only supported on 10G PHYs on port: 2
% Note: Feature  is only supported on 10G PHYs on port: 3
% Note: Feature  is only supported on 10G PHYs on port: 4
% Note: Feature  is only supported on 10G PHYs on port: 5
% Note: Feature  is only supported on 10G PHYs on port: 6
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
% Note: Feature  is only supported on 10G PHYs on port: 14
% Note: Feature  is only supported on 10G PHYs on port: 15
% Note: Feature  is only supported on 10G PHYs on port: 16
% Error: failed to get Oper-mode
SM12DP2XA#
```

port-security

Show port security.

Syntax

show port-security port [interface (<port_type> [<v_port_type_list>])]

show port-security switch [interface (<port_type> [<v_port_type_list>])]

Parameter

port	Show MAC Addresses learned by Port Security
switch	Show Port Security status.
Interface	
<port_type >	GigabitEthernet
*	All Switches or All ports
Gigabitethernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet

EXAMPLE 1

```
SM12DP2XA# show port-security switch
Users:
L = Limit Control
8 = 802.1X
V = Voice VLAN
Interface              Users  State         MAC Cnt
----------------------  -----  -------------  -------
GigabitEthernet 1/1      ---    No users          0
GigabitEthernet 1/2      ---    No users          0
GigabitEthernet 1/3      ---    No users          0
GigabitEthernet 1/4      ---    No users          0
GigabitEthernet 1/5      ---    No users          0
GigabitEthernet 1/6      ---    No users          0
GigabitEthernet 1/7      ---    No users          0
GigabitEthernet 1/8      ---    No users          0
GigabitEthernet 1/9      ---    No users          0
GigabitEthernet 1/10     ---    No users          0
GigabitEthernet 1/11     ---    No users          0
GigabitEthernet 1/12     ---    No users          0
GigabitEthernet 1/13     ---    No users          0
GigabitEthernet 1/14     ---    No users          0
10GigabitEthernet 1/1    ---    No users          0
10GigabitEthernet 1/2    ---    No users          0
```

EXAMPLE 2

```
SM12DP2XA# show port-security port
GigabitEthernet 1/1
-------------------
MAC Address       VID   State      Added                    Age/Hold Time
-----------------  ----  ----------  -------------------------  -------------
<none>
‘’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’’

GigabitEthernet 1/4
-------------------
MAC Address       VID   State      Added                    Age/Hold Time
-----------------  ----  ----------  -------------------------  -------------
SM12DP2XA#
```

privilege

Display current privilege level.

Syntax

show privilege [| {begin | exclude | include } <LINE>

Parameters

|	Output modifiers
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match
<line>	String to match output lines
<line>	String to match output lines
<line>	String to match output lines

EXAMPLE

```
SM12DP2XA# show privilege
SM12DP2XA#
SM12DP2XA# show privilege
-------------------------------------------
|   The order is as the input sequence and   |
|   the last one has the highest priority.   |
 -------------------------------------------

  privilege line level 5 LINE
```

process

Display ongoing process data.

Syntax

show process list [detail]

show process load

Parameters

list	list
load	load
detail	optionally show thread call stack

EXAMPLE

```
SM12DP2XA# show process list
ID  State SetPrio CurPrio Name                 1sec Load 10sec Load Stack Base Size  Used
--- ----- ------- ------- --------------------- --------- ---------- ---------- ----- -----
DSR N/A       N/A     N/A DSR Context                N/A        N/A        N/A   N/A   N/A
129 Exit        7       7 Telnet CLI 2               N/A        N/A 0x81268c00 65536  4688
132 Exit        7       7 SSH Child 1                N/A        N/A 0x8288a370 16384  9568
133 Exit        7       7 SSH CLI 1                  N/A        N/A 0x82847c90 65536  6560
  3 Sleep       6       6 Network alarm support       N/A        N/A 0x832e54d0  4096  1808
  4 Sleep       7       7 Network support             N/A        N/A 0x832e3d40  5328  2312
  5 Susp       15      15 pthread.00000800            N/A        N/A 0x832fa1c8  7828   292
  6 Sleep       7       7 Main                       N/A        N/A 0x826c86d4 16384  1628
  7 Sleep       7       7 Critd                      N/A        N/A 0x826de07c  8192   556
-- more --, next page: Space, continue: g, quit: ^C
SM12DP2XA# show process load
Load average(100ms, 1s, 10s):   3%,   4%,   4%
SM12DP2XA#
SM12DP2XA# show process list detail
Version      : SM12DP2XA (standalone) v7.20.0128
Build Date   : 2024-08-29T10:03:21+08:00
Warning: Return addresses are highly unreliable (code seems to be compiled with -O2)
ID  State SetPrio CurPrio Name                 1sec Load 10sec Load Stack Base Size  Used
--- ----- ------- ------- --------------------- --------- ---------- ---------- ----- -----
DSR N/A       N/A     N/A DSR Context                N/A        N/A        N/A   N/A   N/A
  3 Sleep       6       6 Network alarm support       N/A        N/A 0x83465518  4096  1800
#0  0x8072b524
#1  0x8072cf58
#2  0x80740330
#3  0x80728fac
#4  0x80728f80
  4 Sleep       7       7 Network support             N/A        N/A 0x83463d88  5328  2496
#0  0x8072b524
#1  0x8072cc50
#2  0x8073e440
-- more --, next page: Space, continue: g, quit: ^C
```

pvlan

Display PVLAN status.

Syntax

show pvlan [<pvlan_list>]
show pvlan isolation [interface (<port_type> [<plist>])]

Parameters

<range_list>	PVLAN id to show configuration for
isolation	show isolation configuration
interface	List of port type and port ID, ex, Fast 1/1 Gigabit 2/3-5 Gigabit 3/2-4 Tengigabit 4/6
<port_type >	GigabitEthernet
*	All Switches or All ports
Gigabitethernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet

EXAMPLE

```
SM12DP2XA# show pvlan 1
PVLAN ID  Ports
--------  --------------------------------------------------------------------------------
1         GigabitEthernet 1/1, GigabitEthernet 1/2, GigabitEthernet 1/3,
          GigabitEthernet 1/4, GigabitEthernet 1/5, GigabitEthernet 1/6,
          GigabitEthernet 1/7, GigabitEthernet 1/8, GigabitEthernet 1/9,
          GigabitEthernet 1/10, GigabitEthernet 1/11, GigabitEthernet 1/12,
          GigabitEthernet 1/13, GigabitEthernet 1/14, 10GigabitEthernet 1/1,
          10GigabitEthernet 1/2
SM12DP2XA# show pvlan isolation
Port                            Isolation
-------------------------------  ---------
GigabitEthernet 1/1              Disabled
GigabitEthernet 1/2              Disabled
GigabitEthernet 1/3              Disabled
GigabitEthernet 1/4              Disabled
GigabitEthernet 1/5              Disabled
GigabitEthernet 1/6              Disabled
GigabitEthernet 1/7              Disabled
GigabitEthernet 1/8              Disabled
GigabitEthernet 1/9              Disabled
GigabitEthernet 1/10             Disabled
GigabitEthernet 1/11             Disabled
GigabitEthernet 1/12             Disabled
GigabitEthernet 1/13             Disabled
GigabitEthernet 1/14             Disabled
10GigabitEthernet 1/1            Disabled
10GigabitEthernet 1/2            Disabled
SM12DP2XA#
```

qos

Display Quality of Service data.

Syntax

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

Parameters

interface	Interface
<port_type >	GigabitEthernet
*	All switches or All ports
Gigabitethernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet
maps	Global QoS Maps/Tables
qce	QoS Control Entry
storm	Storm policer
wred	Weighted Random Early Discard
cos-dscp	Map for cos to dscp
dscp-classify	Map for dscp classify enable
dscp-cos	Map for dscp to cos
dscp-egress-translation	Map for dscp egress translation
dscp-ingress-translation	Map for dscp ingress translation
<Qce : 1-256>	QCE ID
<port_type_list>	Port list in 1/1-14
<port_type_list>	Port list in 1/1-2

EXAMPLE

```
SM12DP2XA# show qos storm
qos storm:
==========
Unicast  : disabled      10 fps
Multicast: disabled      10 fps
Broadcast: disabled      10 fps
SM12DP2XA# show qos qce
No qce entries found!
SM12DP2XA# show qos maps
qos map dscp-cos:
=================
DSCP      Trust    Cos  Dpl
---------  --------  ---  ---
0  (BE)    disabled  0    0
1         disabled  0    0
2         disabled  0    0
3         disabled  0    0
4         disabled  0    0
5         disabled  0    0
6         disabled  0    0
7         disabled  0    0
8  (CS1)   disabled  0    0
9         disabled  0    0
10 (AF11)  disabled  0    0
11        disabled  0    0
12 (AF12)  disabled  0    0
13        disabled  0    0
14 (AF13)  disabled  0    0
```

```
15        disabled  0    0
16 (CS2)   disabled  0    0
17        disabled  0    0
SM12DP2XA# show qos wred
qos wred:
=========
Group  Queue  Dpl  Mode      Min Fl  Max Dp or Fl
-----  -----  ---  --------  ------  ----------------------
    1      0    1  disabled    0 %    50 % Drop Probability
    1      0    2  disabled    0 %    50 % Drop Probability
    1      0    3  disabled    0 %    50 % Drop Probability
    1      1    1  disabled    0 %    50 % Drop Probability
    1      1    2  disabled    0 %    50 % Drop Probability
    1      1    3  disabled    0 %    50 % Drop Probability
    1      2    1  disabled    0 %    50 % Drop Probability
    1      2    2  disabled    0 %    50 % Drop Probability
    1      2    3  disabled    0 %    50 % Drop Probability
    1      3    1  disabled    0 %    50 % Drop Probability
    1      3    2  disabled    0 %    50 % Drop Probability
    1      3    3  disabled    0 %    50 % Drop Probability
    1      4    1  disabled    0 %    50 % Drop Probability
    1      4    2  disabled    0 %    50 % Drop Probability
    1      4    3  disabled    0 %    50 % Drop Probability
    1      5    1  disabled    0 %    50 % Drop Probability
    1      5    2  disabled    0 %    50 % Drop Probability
    1      5    3  disabled    0 %    50 % Drop Probability
-- more --, next page: Space, continue: g, quit: ^C
SM12DP2XA# show qos qce 1

static qce 1:
=============
 port: 1-16
 key parameters:
  dmac: unicast
  smac: any
  tag:
   type: any
   vid: any
   pcp: any
   dei: any
  inner tag:
   type: untagged
   vid: any
   pcp: any
   dei: any
  frametype: etype any
 action parameters:
  cos: 0
  dpl: default
  dscp: 20 (AF22)
  tag: default
  policy: default
SM12DP2XA#
```

Messages:

% QOS: qce 1 not found

No qce entries found!

radius-server

Display RADIUS Server statistics.

Syntax

show radius-server [statistics]

Parameters

statistics	RADIUS statistics
|	Output modifiers
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match
<LINE>	String to match output lines

EXAMPLE 1

```
SM12DP2XA# show radius-server
Global RADIUS Server Timeout      : 5 seconds
Global RADIUS Server Retransmit   : 3 times
Global RADIUS Server Deadtime     : 0 minutes
Global RADIUS Server Key          :
Global RADIUS Server Attribute 4  :
Global RADIUS Server Attribute 95 :
Global RADIUS Server Attribute 32 :
RADIUS Server #1:
  Host name  : 1.2.3.4
  Auth port  : 1812
  Acct port  : 1813
  Timeout    :
  Retransmit :
  Key        :
RADIUS Server #2:
  Host name  : BobB
  Auth port  : 1813
  Acct port  : 1812
  Timeout    :
  Retransmit :
  Key        : d56a096f24cc4b3186759e650968f22516f2c626eabe38f518ebc798dda3c895e
232d510ec8c30c32a59b97f75db400b679adeb7e1e919831e79442a9f24157c
RADIUS Server #3:
  Host name  : BobB
  Auth port  : 4445
  Acct port  : 4444
  Timeout    : 700 seconds
  Retransmit : 600 times
  Key        : ecc30543b01283726d6ef111282820552a161f81aec7402c33a7fb0b26b81d046
8fb2e6a76349fc653fd826d4901a303ded46d4e7aca8ad452f3ae8e034b2a3a
RADIUS Server #4:
  Host name  : BobB
  Auth port  : 1646
  Acct port  : 1645
  Timeout    :
  Retransmit :
  Key        : c1ea90f43820d86318313b0a3991bf45aa59024063d73305eba5be2ac72ebc9b5
d328c600ee2b7a76d940b31fbf20c812e5a03e7a9e69976c215041da7a02745
SM12DP2XA#
```

EXAMPLE 2

```
SM12DP2XA# show radius-server statistics
Global RADIUS Server Timeout      : 5 seconds
Global RADIUS Server Retransmit   : 3 times
Global RADIUS Server Deadtime     : 0 minutes
Global RADIUS Server Key          :
Global RADIUS Server Attribute 4  :
Global RADIUS Server Attribute 95 :
Global RADIUS Server Attribute 32 :
RADIUS Server #1:
  Host name  : 1.2.3.4
  Auth port  : 1812
  Acct port  : 1813
  Timeout    :
  Retransmit :
  Key        :
RADIUS Server #2:
  Host name  : BobB
  Auth port  : 1813
  Acct port  : 1812
  Timeout    :
  Retransmit :
  Key        : d56a096f24cc4b3186759e650968f22516f2c626eabe38f518ebc798dda3c895e
232d510ec8c30c32a59b97f75db400b679adeb7e1e919831e79442a9f24157c
RADIUS Server #3:
  Host name  : BobB
  Auth port  : 4445
  Acct port  : 4444
  Timeout    : 700 seconds
  Retransmit : 600 times
  Key        : ecc30543b01283726d6ef111282820552a161f81aec7402c33a7fb0b26b81d046
8fb2e6a76349fc653fd826d4901a303ded46d4e7aca8ad452f3ae8e034b2a3a
RADIUS Server #4:
  Host name  : BobB
  Auth port  : 1646
  Acct port  : 1645
  Timeout    :
  Retransmit :
  Key        : c1ea90f43820d86318313b0a3991bf45aa59024063d73305eba5be2ac72ebc9b5
d328c600ee2b7a76d940b31fbf20c812e5a03e7a9e69976c215041da7a02745

RADIUS Server #1 (1.2.3.4:1812) Authentication Statistics:
Rx Access Accepts:                 0   Tx Access Requests:                0
Rx Access Rejects:                 0   Tx Access Retransmissions:          0
Rx Access Challenges:              0   Tx Pending Requests:                0
Rx Malformed Acc. Responses:       0   Tx Timeouts:                       0
Rx Bad Authenticators:             0
-- more --, next page: Space, continue: g, quit: ^C
```

rapid-ring

Display Rapid Ring configuration.

Syntax

show rapid-ring <cr>

Parameters

| Output modifiers

<cr>

EXAMPLE

```
SM12DP2XA# show rapid-ring
Entry Index             : 1
Rapid Ring Role         : Master
Rapid Ring Port 1       : 1
Rapid Ring Port 2       : 2
Rapid Ring Port 1 State   : Discarding
Rapid Ring Port 2 State   : Discarding

Entry Index             : 2
Rapid Ring Role         : Member
Rapid Ring Port 1       : 3
Rapid Ring Port 2       : 4
Rapid Ring Port 1 State   : Discarding
Rapid Ring Port 2 State   : Discarding

Entry Index             : 3
Rapid Ring Role         : Member
Rapid Ring Port 1       : 5
Rapid Ring Port 2       : 6
Rapid Ring Port 1 State   : Discarding
Rapid Ring Port 2 State   : Discarding

Entry Index             : 4
Rapid Ring Role         : Member
Rapid Ring Port 1       : 7
Rapid Ring Port 2       : 8
Rapid Ring Port 1 State   : Discarding
Rapid Ring Port 2 State   : Discarding

,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

Entry Index             : 7
Rapid Ring Role         : Disabled
Rapid Ring Port 1       : 15
Rapid Ring Port 2       : 16
Rapid Ring Port 1 State   : Forwarding
Rapid Ring Port 2 State   : Forwarding

SM12DP2XA#
```

rmon

Display RMON statistics.

Syntax

show rmon alarm [<id_list>]
show rmon event [<id_list>]
show rmon history [<id_list>]
show rmon statistics [<id_list>]

Parameters

alarm	Display the RMON alarm table
event	Display the RMON event table
history	Display the RMON history table
statistics	Display the RMON statistics table
<1~65535>	Alarm/Event/History/Statistics entry list

EXAMPLE

```
SM12DP2XA# show rmon alarm 1

Alarm ID :    1
---------------
     Interval         : 50000
     Variable         : .1.3.6.1.2.1.2.2.1.20.1
     SampleType       : absoluteValue
     Value        : 0
     Startup          : risingOrFallingAlarm
     RisingThrld      : 90000
     FallingThrld     : -8888
     RisingEventIndex  : 999
     FallingEventIndex : 0

SM12DP2XA# show rmon event

Event ID :    1
---------------
     Description    : r1
     Type           : logandtrap
     Community      : public
     LastSent       : Never

SM12DP2XA# show rmon history

History ID :    1
-----------------
    Data Source        : .1.3.6.1.2.1.2.2.1.1.1
    Data Bucket Request : 50
    Data Bucket Granted : 50
    Data Interval      : 1800

SM12DP2XA# show rmon statistics

Statistics ID :    1
--------------------
    Data Source : .1.3.6.1.2.1.2.2.1.1.1
    etherStatsDropEvents         : 0
    etherStatsOctets             : 0
    etherStatsPkts               : 0
    etherStatsBroadcastPkts      : 0
    etherStatsMulticastPkts      : 0
    etherStatsCRCAlignErrors     : 0
```

```
    etherStatsUndersizePkts      : 0
    etherStatsOversizePkts       : 0
    etherStatsFragments          : 0
    etherStatsJabbers            : 0
    etherStatsCollisions         : 0
    etherStatsPkts64Octets       : 0
    etherStatsPkts65to127Octets  : 0
    etherStatsPkts128to255Octets : 0
    etherStatsPkts256to511Octets : 0
    etherStatsPkts512to1023Octets : 0
    etherStatsPkts1024to1518Octets: 0
SM12DP2XA#
```

running-config

Show running system information.

Syntax

show running-config [all-defaults]
show running-config feature <feature_name> [all-defaults]
show running-config interface (<port_type> [<list>]) [all-defaults]
show running-config interface vlan <list> [all-defaults]
show running-config line { console | vty } <list> [all-defaults]
show running-config vlan { [<vlan_list>] } [all-defaults]

Parameters

all-defaults	Include most/all default values
feature	Show configuration for specific feature
interface	Show specific interface(s)
line	Show line settings
vlan	VLAN
<cword>	Valid words are 'GVRP' 'R-Ring' 'access' 'access-list' 'aggregation' 'arp-inspection' 'auth' 'broadcast-storm-protection' 'cli_telnet' 'clock' 'dhcp' 'dhcp-snooping' 'dhcp6_client_interface' 'dhcp_server' 'dms-server' 'dns' 'dot1x' 'green-ethernet' 'http' 'icli' 'ip-igmp-snooping' 'ip-igmp-snooping-port' 'ip-igmp-snooping-vlan' 'ipmc-profile' 'ipmc-profile-range' 'ipv4' 'ipv6' 'ipv6-mld-snooping' 'ipv6-mld-snooping-port' 'ipv6-mld-snooping-vlan' 'lacp' 'lldp' 'logging' 'loop-protect' 'mac' 'mstp' 'mvr' 'mvr-port' 'ntp' 'phy' 'port' 'port-security' 'push_notification' 'pvlan' 'qos' 'rmon' 'sflow' 'smtp' 'snmp' 'source-guard' 'ssh' 'sysutil' 'trap_event' 'udld' 'upnp' 'user' 'vlan' 'voice-vlan' 'vtss-rmirror' 'vtun' 'web' 'web-privilege-group-level'
<port_type >	GigabitEthernet
*	All switches or All ports
Gigabitethernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet
<vlan_list>	List of VLAN numbers
console	Console
vty	VTY
<range_list>	List of console/VTYs

EXAMPLE

```
SM12DP2XA# show running-config
Building configuration...
hostname SM12DP2XA
username admin privilege 15 password encrypted YWRtaW4=
ip dhcp server
ip dhcp excluded-address 200.100.0.0 200.100.0.10
!
vlan 10
 name VID10
!
vlan 1,20,30,50
!
!
ipmc profile Prof-1
 description profileOne
!
ipmc profile
```

```
!
snmp-server host SnmpTrap-1
 no shutdown
 host 192.168.1.30 162 informs
 version v3 probe None
!
snmp-server host SnmpTrap-2
 no shutdown
 host 192.168.1.40 162 informs
!
snmp-server host Trapv1
 no shutdown
 host 192.168.1.50 162 traps
 version v1 public
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
vlan protocol eth2 ip group grp1
ip arp inspection
ip source binding interface GigabitEthernet 1/2 10 192.168.1.77 00-c0-f2-49-38-b
b
clock timezone test 8
tzidx 2
mac address-table aging-time 0
mac address-table static 00:00:00:00:00:00 vlan 1 interface GigabitEthernet 1/2
spanning-tree mode stp
spanning-tree mst hello-time 4
spanning-tree transmit hold-count 8
spanning-tree recovery interval 70000
spanning-tree mst name Charlie revision 1
spanning-tree mst 1 vlan 10
spanning-tree mst 2 vlan 20-40,90
qos storm unicast 12345678 fps
qos storm multicast 99999 fps
qos storm broadcast 5 kfps
qos wred group 1 queue 0 dpl 2 min-fl 0 max 50
qos wred group 1 queue 1 dpl 3 min-fl 0 max 50 fill-level
access-list ace 5 frame-type etype etype-value 0xabcd
voice vlan
voice vlan class 5
voice vlan oui 00-01-E3 description Siemens AG phone
voice vlan oui 00-E0-75 description Polycom/Veritel phone
dot1x re-authentication
dot1x system-auth-control
system name SM12DP2XA
system description Managed Switch, (12) 100/1000Base-X SFP ports + (2) 1G/10G SF
P+ with (2) 10/100/1000Base-T
!
interface GigabitEthernet 1/1
```

```
-- more --, next page: Space, continue: g, quit: ^C
```

sflow

Display Statistics flow (sFlow) data.

Syntax

show sflow statistics { receiver [<rcvr_idx_list>] | samplers [interface [<samplers_list>] (<port_type> [<v_port_type_list>])] }

Parameters

statistics	sFlow statistics.
receiver	Show statistics for receiver.
samplers	Show statistics for samplers.
<range_list>	runtime, see sflow_icli_functions.c
<port_type >	GigabitEthernet
*	All switches or All ports
Gigabitethernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet
|	Output modifiers

EXAMPLE

```
SM12DP2XA# show sflow
Agent Configuration:
====================
Agent Address: 127.0.0.1
Receiver Configuration:
=======================
Owner       : <none>
Receiver    : 0.0.0.0
UDP Port    : 6343
Max. Datagram: 1400 bytes
Time left   : 0 seconds
No enabled collectors (receivers). Skipping displaying per-port info.
SM12DP2XA# show sflow statistics ?
   receiver   Show statistics for receiver.
   samplers   Show statistics for samplers.
SM12DP2XA# show sflow statistics receiver ?
   |      Output modifiers
   <cr>
SM12DP2XA# show sflow statistics receiver
Tx Successes     Tx Errors       Flow Samples     Counter Samples
--------------  --------------  ---------------  ---------------
            0               0              0               0
SM12DP2XA#
```

smtp

Display SMTP parameters.

Syntax

show smtp

EXAMPLE

```
SM12DP2XA# show smtp
Mail Server     : 192.168.1.77
User Name       : jeffs
Password        : ********
Sender          : smtp1
Return Path     : sm12@hotmail.com
Email Adress 1  : jeffs@transition.com
Email Adress 2  : support@transition.com
Email Adress 3  :
Email Adress 4  :
Email Adress 5  :
Email Adress 6  :
SM12DP2XA#
```

snmp

Display SNMP parameters.

Syntax

show snmp
show snmp access [<group_name> { v1 | v2c | v3 | any } { auth | noauth | priv }]
show snmp community v3 [<community>]
show snmp host [<conf_name>] [system] [switch] [interface] [aaa]
show snmp info
show snmp mib context
show snmp mib ifmib ifIndex
show snmp security-to-group [{ v1 | v2c | v3 } <security_name>]
show snmp user [<username> <engineID>]
show snmp view [<view_name> <oid_subtree>]

Parameters

access	access configuration
<GroupName : word32>	Group name
v1	v1 security model
v2c	v2c security model
v3	v3 security model
any	any security model
auth	authNoPriv Security Level
noauth	noAuthNoPriv Security Level
priv	authPriv Security Level
community	Community
v3	SNMPv3
<Community : word127>	Specify community name
host	Set SNMP host's configurations
<ConfName : word32>	Name of the host configuration
system	System event group
switch	Switch event group
interface	Interface event group
aaa	AAA event group
mib	MIB (Management Information Base)
security-to-group	security-to-group configuration
<SecurityName : word32>	security group name
user	User
<UserName : word32>	Security user name
<EngineId : word10-32>	Security Engine ID
view	MIB view configuration
<ViewName : word32>	MIB view name
<OidSubtree : word255>	MIB view OID
<word32>	Name of the host configuration
aaa	AAA event group
interface	Interface event group
switch	Switch event group
system	System event group

EXAMPLE 1

```
SM12DP2XA# show snmp

SNMP Configuration
SNMP Mode                    : enabled
SNMP Version                 : 2c
Read Community               : public
Write Community              : private
Trap Mode                    : disabled

SNMPv3 Communities Table:
Community   : public
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0

Community   : private
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0


SNMPv3 Users Table:
User Name              : default_user
Engine ID              : 800007e5017f000001
Security Level          : NoAuth, NoPriv
-- more --, next page: Space, continue: g, quit: ^C
```

EXAMPLE 2

```
SM12DP2XA# show snmp access
Group Name       : default_ro_group
Security Model   : any
Security Level   : NoAuth, NoPriv
Read View Name   : default_view
Write View Name  : <no writeview specified>

Group Name       : default_rw_group
Security Model   : any
Security Level   : NoAuth, NoPriv
Read View Name   : default_view
Write View Name  : default_view

SM12DP2XA#
```

EXAMPLE 3

```
SM12DP2XA# show snmp community v3
Community   : WComm
Source IP   : 1.2.3.4
Source Mask : 255.255.255.0

Community   : public
Source IP   : 0.0.0.0
```

```
Source Mask : 0.0.0.0

Community   : private
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0

SM12DP2XA#
```

EXAMPLE 4

```
SM12DP2XA# show snmp host aaa
Trap Global Mode: disabled
Trap ShostOne (ID:0) is enabled
Community       : public
Destination Host: 0.0.0.0
UDP Port        : 162
Version         : V3
Inform Mode     : disabled
Inform Timeout  : 125
Inform Retry    : 50
Probe Mode      : enabled
Engine ID       :
Security Name   : seucrityname

SM12DP2XA# show snmp info

SNMP Info:
Conf VendorName:TN, VENDOR_GENERIC, PRODUCT:SM12DP2XA
EngineID: 800007e5017f000001
Using     oid :1.3.6.1.4.1.868.2.76, length:9
SM12DP2XA#
```

spanning-tree

Display STP Bridge.

Syntax

show spanning-tree [summary | active | { interface (<port_type> [<v_port_type_list>]) } | { detailed [interface (<port_type> [<v_port_type_list_1>])] } | { mst [configuration | { <instance> [interface (<port_type> [<v_port_type_list_2>])] }] }]

Parameters

summary	STP summary
active	STP active interfaces
interface	Choose port
<port_type>	* or Gigabitethernet
*	All switches or All ports
Gigabitethernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet
detailed	STP statistics
interface	List of port type and port ID, ex, 1/1-14
mst	Configuration
configuration	STP bridge instance no (0-7, CIST=0, MST2=1...)
<0-7>	Choose port

EXAMPLE

```
SM12DP2XA# show spanning-tree
CIST Bridge STP Status
Bridge ID    : 32768.00-C0-F2-49-38-BB
Root ID      : 32768.00-C0-F2-49-38-BB
Root Port    : -
Root PathCost: 0
Regional Root: 32768.00-C0-F2-49-38-BB
Int. PathCost: 0
Max Hops     : 20
TC Flag      : Steady
TC Count     : 0
TC Last      : -
Port       Port Role       State       Pri  PathCost  Edge  P2P  Uptime
---------  --------------  ----------  ---  --------  ----  ---  -------------
Gi 1/14    DesignatedPort  Forwarding  128     20000  Yes   Yes    0d 19:00:08
SM12DP2XA# show spanning-tree summary
Protocol Version: MSTP
Hello Time      : 2
Max Age         : 20
Forward Delay   : 15
Tx Hold Count   : 6
Max Hop Count   : 20
BPDU Filtering  : Disabled
BPDU Guard      : Disabled
Error Recovery  : Disabled
CIST Bridge is active
SM12DP2XA#
```

switchport

Display switching mode characteristics.

Syntax

show switchport forbidden [{ vlan <vlan_list> } | { name <name> }]

Parameters

forbidden	Lookup VLAN Forbidden port entry.
name	name - Show forbidden access for specific VLAN name.
vlan	vid - Show forbidden access for specific VLAN id.
<vlan_id>	VLAN id
<word31>	VLAN name

EXAMPLE

```
SM12DP2XA# show switchport forbidden
VLAN  Name                            Interfaces
----  ------------------------------  ----------
10    VID10                           Gi 1/2
20    VLAN0020                        Gi 1/3
30    VLAN0030                        Gi 1/4
SM12DP2XA# show switchport forbidden vlan 1-15
VLAN  Name                            Interfaces
----  ------------------------------  ----------
1     default
2     VLAN0002                        Gi 1/2
3     VLAN0003
4     VLAN0004
5     VLAN0005
6     VLAN0006
7     VLAN0007
8     VLAN0008
9     VLAN0009
10    VLAN0010                        Gi 1/2
11    VLAN0011                        Gi 1/2
12    VLAN0012                        Gi 1/2
13    VLAN0013                        Gi 1/2
14    VLAN0014
15    VLAN0015                        Gi 1/2
SM12DP2XA#
```

Messages:

% VLAN name does not exist

% No forbidden VLANs found

system

Show system information.

Syntax

show system cpu | reboot | <cr>

Parameters

show system <cr>
show system cpu status
show system reboot

EXAMPLE

```
SM12DP2XA# show system <cr>
Model Name                  : SM12DP2XA
System Description          : Managed Switch, (12) 100/1000Base-X SFP ports + (2) 1G/10G SFP+ with (2)
10/100/1000Base-T
Location                    :
Contact                     :
System Name                 : SM12DP2XA
System Date                 : 2024-08-16T09:44:22+00:00
System Uptime               : 2d 18:31:02
Bootloader Version          : v0.5
Firmware Version            : v7.20.0208 2024-08-14
Hardware Version            : v1.01
Mechanical Version          : v1.01
Serial Number               : A076118AR0900004
MAC Address                 : 00-c0-f2-49-38-ee
Memory                      : Total=73438 KBytes, Free=50258 KBytes, Max=50041 KBytes
FLASH                       : 0x40000000-0x41ffffff, 512 x 0x10000 blocks
Fan Speed                   : 5726(rpm)
Power Source                : AC
Powers                      : AC Power On 13.50V ; DC Power On 0.00V
Temperature 1               : 31(C) ; 87(F)
Temperature 2               : 26(C) ; 78(F)
SM12DP2XA#
SM12DP2XA# SM12DP2XA# show system cpu status
    Average load in 100 ms  : 0%
    Average load in   1 sec : 3%
    Average load in  10 sec : 4%
SM12DP2XA# show system reboot
Switch Reboot Mode: Disable
Switch Reboot Entry:
            Reboot Time
  Week Day     HH : MM
 ----------    -------
  Monday        -  -
  Tuesday       -  -
  Wednesday     -  -
  Thursday      -  -
  Friday        -  -
  Saturday      -  -
  Sunday        -  -
SM12DP2XA#
```

tacacs-server

Display TACACS+ configuration.

Syntax

show tacacs-server [| {begin | exclude | include } <LINE>

Parameters

|	Output modifiers
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match

EXAMPLE

```
SM12DP2XA# show tacacs-server
Global TACACS+ Server Timeout      : 300 seconds
Global TACACS+ Server Deadtime     : 0 minutes
Global TACACS+ Server Key          : 0fca8039dbafe251c1cc91b37b65d2255a90008afa4
645157aa8a3e6137d6f92a0be0ad395c0188db281522a4624273eac45b7bb83980a577b303cdff90
6b2ae
TACACS+ Server #1:
  Host name  : 1.2.3.4
  Port       : 555
  Timeout    : 300 seconds
  Key        : 56009e57d57329db4fd1d8afeee7d8d7952543e776dfb0f2c450a6604c43981f0
7be81bf2393b5e655243889d8fb48b0fb08160432a735de83cc26ae9f6451a4
TACACS+ Server #2:
  Host name  : ip
  Port       : 49
  Timeout    :
  Key        :
SM12DP2XA#
```

terminal

Display terminal configuration parameters.

Syntax

show terminal [| {begin | exclude | include } <LINE>

Parameters

|	Output modifiers
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match
<LINE>	String to match output lines

EXAMPLE

```
SM12DP2XA# show terminal
Line is vty 0.
    * You are at this line now.
    Alive from Telnet.
    Default privileged level is 2.
    Command line editing is enabled
    Display EXEC banner is enabled.
    Display Day banner is enabled.
    Terminal width is 80.
            length is 24.
            history size is 32.
            exec-timeout is 1440 min 0 second.

    Current session privilege is 15.
    Elapsed time is 0 day 1 hour 1 min 35 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

SM12DP2XA#
```

show udld

Display Unidirectional Link Detection (UDLD) configuration, statistics and status.

Syntax

show udld [interface (<port_type> [<plist>])]

Parameters

|	Output modifiers
interface	Choose port
*	All switches or All ports
GigabitEthernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list for all port types
<port_type_list>	Port list in 1/1-14
<port_type_list>	Port list in 1/1-2

EXAMPLE

```
SM12DP2XA# show udld interface 10GigabitEthernet 1/1-2

10GigabitEthernet 1/1
--------------------------------------------------------------------
UDLD Mode               : Disable
Admin State             : Disable
Message Time Interval(Sec): 7
Device ID(local)         : 00-C0-F2-49-38-DD
Device Name(local)       : SM12DP2XA
Bidirectional state      : Indeterminant

No neighbor cache information stored
---------------------

10GigabitEthernet 1/2
--------------------------------------------------------------------
UDLD Mode               : Disable
Admin State             : Disable
Message Time Interval(Sec): 7
Device ID(local)         : 00-C0-F2-49-38-DD
Device Name(local)       : SM12DP2XA
Bidirectional state      : Indeterminant

No neighbor cache information stored
---------------------
SM12DP2XA#
```

upnp

Display Universal Plug and Play configuration.

Syntax

show upnp [| {begin | exclude | include } <LINE>

Parameters

|	Output modifiers
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match
<LINE>	String to match output lines

EXAMPLE

```
SM12DP2XA# show upnp
UPnP Mode                : disabled
UPnP TTL                 : 4
UPnP Advertising Duration : 100
SM12DP2XA# show upnp
UPnP Mode                : enabled
UPnP TTL                 : 50
UPnP Advertising Duration : 5000
SM12DP2XA#
```

user-privilege

Display Users privilege configuration.

Syntax

show user-privilege <cr>

Parameters

user-privilege	Users privilege configuration
<cr>	

EXAMPLE

```
SM12DP2XA# show user-privilege
username admin privilege 15 password encrypted
1e40ff6b7983136e48112794162b14068d61a78e0aae8b38a9cea974014df70acc7bafa3d8df701a3a755d5395be687cbc82a
59d0114a757191ae411b0f8f2b6
SM12DP2XA# show user-privilege
username BobB privilege 14 password encrypted e0155680a485c4baed83de249a5f45d3d3
9d2d4e1fbde1fc45b35bba248e8e2837164618d235eb3acaf089ccbf028989d3fa3426afac7ad73d
f622bc801f0bb1
username admin privilege 15 password encrypted 125d0967b8555a155d7f585559427cb98
a0d3e62ac4d7fa8adb9c154a3654e8a9aef00c89443f57dbdbd29fc474818300ceab9d5a2a7a8b35
f924091fdf23b3e
SM12DP2XA#
```

users

Display information about terminal lines.

Syntax

show users myself [| {begin | exclude | include } <LINE>

Parameters

myself	Display information about mine
|	Output modifiers
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match
<LINE>	String to match output lines

EXAMPLE

```
SM12DP2XA# show users
Line is vty 0.
    * You are at this line now.
    Connection is from 192.168.1.99:62239 by Telnet.
    User name is admin.
    Privilege is 15.
    Elapsed time is 0 day 0 hour 0 min 33 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

SM12DP2XA#
```

version

Show system hardware and software status.

Syntax

show version

show version [brief]

Parameters

|	Output modifiers
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match
<LINE>	String to match output lines
brief	show just version and build date

EXAMPLE

```
SM12DP2XA# show version brief
Version      : SM12DP2XA (standalone) v7.20.0208
Build Date   : 2024-08-14T17:56:47+08:00
SM12DP2XA# show version

MEMORY          : Total=73438 KBytes, Free=50258 KBytes, Max=50041 KBytes
FLASH           : 0x40000000-0x41ffffff, 512 x 0x10000 blocks
MAC Address     : 00-c0-f2-49-38-ee
Previous Restart : Warm

System Contact   :
System Name      : SM12DP2XA
System Location  :
System Time      : 2023-10-16T09:46:08+00:00
System Uptime    : 2d 18:32:48

Active Image
------------
Image           : managed
Version         : SM12DP2XA (standalone) v7.20.0208
Date            : 2024-08-14T17:56:47+08:00

Alternate Image
---------------
Image           : managed.bk
Version         : SM12DP2XA (standalone) v7.20.0206
Date            : 2022-03-10T18:38:11+08:00

SM12DP2XA#
```

vlan

Show VLAN parameters.

Syntax

show vlan [id <vlan_list> | name <name> | brief] [all]

show vlan ip-subnet [<ipv4>]

show vlan mac [address <mac_addr>]

show vlan membership [id <vlan_list> | name <name>] [admin | combined | erps | evc | gvrp | mep | mstp | mvr | nas | rmirror | vcl | voice-vlan | dms | mrp | forbidden]

show vlan protocol [eth2 { <etype> | arp | ip | ipx | at }] [snap { <oui> | rfc-1042 | snap-8021h } <pid>] [llc <dsap> <ssap>]

show vlan status [interface (<port_type> [<plist>])] [admin | all | combined | conflicts | erps | evc | gvrp | mep | mstp | mvr | nas | rmirror | vcl | voice-vlan]

Parameters

all	Show all VLANs (if left out only access VLANs are shown)
brief	VLAN summary information
id	VLAN status by VLAN id
ip-subnet	Show VCL IP Subnet entries.
mac	Show VLAN MAC entries.
membership	VLAN membership
name	VLAN status by VLAN name
protocol	Protocol-based VLAN status
status	Show the VLANs configured for each interface.
<vlan_list>	VLAN IDs 1-4095
<vword32>	A VLAN name
eth2	Ethernet protocol based VLAN status
<0x600-0xffff>	Ether Type(Range: 0x600 - 0xFFFF)
arp	Ether Type is ARP
ip	Ether Type is IP
ipx	Ether Type is IPX
at	Ether Type is AppleTalk
snap	SNAP-based VLAN status
<0x0-0xffffff>	SNAP OUI (Range 0x000000 - 0XFFFFFF)
rfc_1042	SNAP OUI is rfc_1042
snap_8021h	SNAP OUI is 8021h
<0x0-0xffff>	PID (Range: 0x0 - 0xFFFF)
llc	LLC-based VLAN status
<0x0-0xff>	DSAP (Range: 0x00 - 0xFF)
<0x0-0xff>	SSAP (Range: 0x00 - 0xFF)
admin	Show the VLANs configured by administrator.
combined	Show the VLANs configured by a combination.
gvrp	Show the VLANs configured by GVRP.
interface	Show the VLANs configured for a specific interface(s).
mstp	Show the VLANs configured by MSTP.
mvr	Show the VLANs configured by MVR.
nas	Show the VLANs configured by NAS.
voice-vlan	Show the VLANs configured by Voice VLAN.
dms	Show the VLANs configured by DMS.
forbidden	Show VLANs configurations that has forbidden.
id	VLAN membership by VLAN id
name	VLAN membership by VLAN name
rmirror	Show the VLANs configured by Remote mirroring.
interface	Show the VLANs configured for a specific interface(s).
<port_type >	GigabitEthernet
Gigabitethernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet
<ipv4_subnet>	Specify a specific IP Subnet.
address	Show a specific MAC entry.
<mac_ucast>	The specific MAC entry to show.

EXAMPLE

```
SM12DP2XA# show vlan brief
VLAN  Name                            Interfaces
----  --------------------------------  ----------
1     default                         Gi 1/1-14 10G 1/1-2

SM12DP2XA# show vlan
VLAN  Name                            Interfaces
----  --------------------------------  ----------
1     default                         Gi 1/1-5,7-14 10G 1/1-2
10    VLAN0010                        Gi 1/3-5
20    VLAN0020                        Gi 1/3-5
30    VLAN0030                        Gi 1/3-5
40    VLAN0040                        Gi 1/3-6

SM12DP2XA# show vlan membership
VLAN  Name                            User Type   Interfaces
----  --------------------------------  ----------  ----------
1     default                         Admin      Gi 1/1-5,7-14 10G 1/1-2
2     VLAN0002                        Admin      Gi 1/3-5
3     VLAN0003                        Admin      Gi 1/3-5
4     VLAN0004                        Admin      Gi 1/3-5
5     VLAN0005                        Admin      Gi 1/3-5
6     VLAN0006                        Admin      Gi 1/3-5
7     VLAN0007                        Admin      Gi 1/3-5
8     VLAN0008                        Admin      Gi 1/3-5
9     VLAN0009                        Admin      Gi 1/3-5
10    VLAN0010                        Admin      Gi 1/3-5
11    VLAN0011                        Admin      Gi 1/3-5
12    VLAN0012                        Admin      Gi 1/3-5
-- more --, next page: Space, continue: g, quit: ^C
SM12DP2XA# show vlan mac address 00-c0-f2-49-38-dd
Entry with MAC address 00-c0-f2-49-38-dd was not found in the switch/stack
SM12DP2XA#
```

voice

Display Voice appliance attributes.

Syntax

show voice vlan [oui <oui> | interface (<port_type> [<port_list>])]

Parameters

vlan	Vlan for voice traffic
oui	OUI configuration
<oui>	OUI value
interface	Select an interface to configure
<port_type>	* or Gigabitethernet
*	All Switches or All ports
Gigabitethernet	1 Gigabit Ethernet Port
10GigabitEthernet	10 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-14 for Gigabitethernet, Port list in 1/1-2 for 10Gigabitethernet
<port_type_list>	Port list for all port types

EXAMPLE

```
SM12DP2XA# show voice vlan
Switch voice vlan is disabled
Switch voice vlan ID is 1000
Switch voice vlan aging-time is 86400 seconds
Switch voice vlan traffic class is 7

Telephony OUI  Description
-------------  -----------

Voice VLAN switchport is configured on following:

GigabitEthernet 1/1 :
---------------------
GigabitEthernet 1/1 switchport voice vlan mode is disabled
GigabitEthernet 1/1 switchport voice security is disabled
GigabitEthernet 1/1 switchport voice discovery protocol is oui

GigabitEthernet 1/2 :
---------------------
GigabitEthernet 1/2 switchport voice vlan mode is disabled
GigabitEthernet 1/2 switchport voice security is disabled
GigabitEthernet 1/2 switchport voice discovery protocol is oui

-- more --, next page: Space, continue: g, quit: ^C
SM12DP2XA# show voice vlan oui FC:EC:DA
Telephony OUI  Description
-------------  -----------
SM12DP2XA#
```

web

Display web privilege information.

Syntax

show web privilege group [<group_name>] level

Parameters

privilege	Web privilege		
group	Web privilege group		
CWORD	Valid words are:		
Aggregation	DHCP	DHCPv6_Client	DMS_client
DMS_server	Debug	Diagnostics	IP
IPMC_Snooping	Install_Wizard	LACP	LLDP
NTP	Ports	Private_VLANs	QoS
RMirror	R_RING	SMTP	Security
Spanning_Tree	System	TS_client	TS_server
Trap_Event	Trouble_Shooting	UDLD	UPnP
VCL	VLANs	VTUN	Voice_VLAN
XXRP	Percepxion	sFlow	
level	Web privilege group level (0-15)		

EXAMPLE

```
SM12DP2XA# show web privilege group level
Group Name                      Privilege Level
                               CRO CRW SRO SRW
------------------------------- --- --- --- ---
Aggregation                      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
DMS_client                       5  10   5  10
DMS_server                       5  10   5  10
Install_Wizard                   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
MVR                              5  10   5  10
NTP                              5  10   5  10
Ports                            5  10   1  10
-- more --, next page: Space, continue: g, quit: ^C
SM12DP2XA# show web privilege group QoS level
Group Name                      Privilege Level
                               CRO CRW SRO SRW
------------------------------- --- --- --- ---
QoS                              5  10   5  10
SM12DP2XA#
```

22. Terminal Commands

Set terminal line parameters.

Syntax

terminal editing
terminal exec-timeout <min> [<sec>]
terminal help
terminal history size <history_size>
terminal length <lines>
terminal width <width>

Parameters

editing	Enable command line editing
exec-timeout	Set the EXEC timeout
help	Description of the interactive help system
history	Control the command history function
length	Set number of lines on a screen
width	Set width of the display terminal
<0-1440>	Timeout in minutes
<0-3600>	Timeout in seconds
size	Set history buffer size
<0-32>	Number of history commands, 0 means disable
<0,3-512>	Number of lines on screen (0 for no pausing)
<0,40-512>	Number of characters on a screen line (0 for unlimited width)

EXAMPLE

```
SM12DP2XA# terminal exec-timeout 1440
SM12DP2XA# terminal help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)

SM12DP2XA#
```

23. Traceroute Commands

traceroute

Run traceroute program.

SYNTAX

traceroute ip <v_ip_addr> [protocol { icmp | udp | tcp }] [wait <v_wait_time>] [ttl <v_max_ttl>] [nqueries <v_nqueries>]

Parameters

ip	IP
<word1-255>	destination address
nqueries	Specify number of probe packets
<1-10>	1-10; Default is 3
protocol	Specify protocol including icmp, udp and tcp
icmp	icmp/udp/tcp; Default is icmp
tcp	Usee TCP protocol
udp	Use UDP protocol
ttl	Specify max TTL
wait	Specify wait time
<1-255>	1-255; Default is 30
<1-60>	1-60 sec; Default is 5 sec

EXAMPLE

```
SISPM1040-384-LRT-C# traceroute ip 192.168.1.77 nqueries 2 protocol tcp ttl 10 wait 20
traceroute to 192.168.1.77 (192.168.1.77), 10 hops max, 40 byte packets
 1 192.168.90.1  (192.168.90.1)  3 ms  1 ms
 2 172.16.44.254  (172.16.44.254)  1 ms  0 ms
 3 192.168.1.77  (192.168.1.77)  1 ms  1 ms
SISPM1040-384-LRT-C#
SISPM1040-384-LRT-C# $ceroute ip 22 nqueries 4 protocol tcp ttl 15 wait 20
traceroute: unknown host 22
SISPM1040-384-LRT-C#
```

24. Troubleshooting and Support

Troubleshooting

Most problems are caused by the following situations. Check for these items first when starting your troubleshooting:

1. Make sure your switch model supports the feature or function attempted; see chapter 1.
2. Verify the install process; see chapter 2.
3. Troubleshoot connected network devices to pinpoint the problem to the switch.
4. Make sure you are in the correct CLI mode for the CLI command you are entering.
5. Connecting to devices that have a fixed full- duplex configuration. Make sure all devices connected to the SM12DP2XA Switch devices are configured to auto negotiate, or are configured to connect at half duplex.
6. Faulty or loose cables. Look for loose or obviously faulty connections. If they appear to be OK, make sure the connections are snug. If that does not correct the problem, try a different cable.
7. Non-standard cables. Non-standard and miswired cables may cause network collisions and other network problems, and can seriously impair network performance. Use a new correctly-wired cable. A cable tester is a recommended tool for every Ethernet network installation.
8. Improper Network Topologies. It is important to make sure you have a valid network topology. If you no longer experience the problems, the new topology is probably at fault. In addition, you should make sure that your network topology contains no data path loops.
9. Check the port configuration. A port on your Switch may not be operating as you expect because it has been put into a “blocking” state by Spanning Tree, GVRP (automatic VLANs), or LACP (automatic trunking). (Note that the normal operation of the Spanning Tree, GVRP, and LACP features may put the port in a blocking state.) Or, the port just may have been configured as disabled through software.
10. SYS LED is Off. Check connections between the switch, the power cord and the wall outlet. Contact Tech Support for assistance.
11. Link LED is Off. Verify that the switch and attached device are powered on. Be sure the cable is plugged into the switch and corresponding device. If the switch is installed in a rack, check the connections to the punch-down block and patch panel. Verify that the proper cable type is used and its length does not exceed specified limits. Check the adapter on the attached device and cable connections for possible defects. Replace the defective adapter or cable if necessary.
12. Contact Tech Support for assistance.

Recording Device and System Information

After performing the troubleshooting procedures, and before calling or emailing Technical Support, please record as much information as possible in order to help the Tech Support Specialist.

1. Select the SM12DP2XA **Monitor** > **System** > **Information** menu path. From the CLI, use the **show** commands needed to gather the information below or as requested by the TN Support Specialist.
2. Record SM12DP2XA **Model Information**: Model Name: _____
   Hardware Version: _____ Mechanical Version: _____
   Firmware Version: _____ System Date: _____
3. Record the **LED** Status: _____
   _____
4. Provide additional information to your Tech Support Specialist. See the "Troubleshooting" section above.

Your Lantronix service contract number: _____

Describe the failure: _____
_____
_____

Describe any action(s) already taken to resolve the problem (e.g., changing mode, rebooting, etc.):
_____
_____
_____

The serial and revision numbers of all involved Lantronix products in the network:
_____
_____

Describe your network environment (layout, cable type, etc.): _____
_____
_____

Network load and frame size at the time of trouble (if known): _____

The device history (i.e., have you returned the device before, is this a recurring problem, etc.): _____
_____
_____
_____

Any previous Return Material Authorization (RMA) numbers: _____

Appendix A. DHCP Per Port

Configure DHCP Per Port via the CLI

The switch's DHCP server assigns IP addresses. Clients get IP addresses in sequence and the switch assigns IP addresses to on a per-port basis starting from the configured IP range. For example, if the IP address range is configured as 192.168.10.20 - 192.168.10.37 with one DHCP device connected to port 1, the client will always get IP address 192.168.10.20, then port 3 is always distributed IP address 192.168.10.22, even if port 2 is an empty port (because port 2 is always distributed IP address 192.168.10.21).

The switch does not allow a DHCP per Port pool to include the switch's address. IP address assigned range and VLAN 1 should stay in the same subnet mask. The configurable IP address range is allowed to configure over 18 IP addresses, but the switch always assigns one IP address per port connecting device.

When the DHCP Per Port function is enabled, the switch software will automatically create the related DHCP pool named "DHCP_Per _Port". Once the DHCP Per Port function is enabled on one switch, IPv4 DHCP client at VLAN1 mode (DMS DHCP mode), DHCP server mode are all limited to be enabled at the same time (an error message displays if attempted). If the DHCP server pool has been configured, once you enable the DHCP Per port function that DHCP server pool configuration will be overwritten.

Only for VLAN 1, clients issued DHCP packets will not be broadcast/forwarded to other ports. DHCP packets in others VLANs will be broadcast/forwarded to others ports.

The DHCP Per Port function allows the switch to connect only one DHCP client device.

The DHCP Per Port function is confiured and shown using these CLI commands:

```
# show ip dhcp server
(config)# ip dhcp server per-port
(config)# no ip dhcp server per-port
```

The CLI commands to configure and show DHCP Per Port are described below.

Command: Show the current DHCP Server and DHCP Per Port configuration

Syntax: show ip dhcp server <cr>

Description: Show if DHCP server is globally enabled or disabled, if all VLANs are disabled or enabled, and if the DHCP server Per Port function is disabled or enabled.

Example: Display the current DHCP Server and Per Port configuration, change the config, and display the results:

```
SM12DP2XA(config)# do show ip dhcp server
DHCP server is globally enabled.
Enabled VLANs are 1.
DHCP server per port is disabled.
SM12DP2XA(config)# ip dhcp server per-port
SM12DP2XA(config)# do show ip dhcp server
DHCP server is globally enabled.
Enabled VLANs are 1.
DHCP server per port is enabled.
SM12DP2XA(config)# no ip dhcp server per-port
SM12DP2XA(config)# do show ip dhcp server
DHCP server is globally enabled.
Enabled VLANs are 1.
DHCP server per port is disabled.
```

```
SM12DP2XA(config)#
```

Command: Configure the DHCP Per Port function

Syntax: ip dhcp server per-port <cr>

Description: Toggle the DHCP Per Port function from Diasbled (default) to Enabled.

Example: Toggle the DHCP Per Port function and show the resulting config:

```
SM12DP2XA# show ip dhcp server
DHCP server is globally disabled.
All VLANs are disabled.
SM12DP2XA# con ter
SM12DP2XA(config)# ip dhcp ?
excluded-address Prevent DHCP from assigning certain addresses
pool Configure DHCP address pools
relay DHCP relay agent configuration
server Enable DHCP server
snooping DHCP snooping
SM12DP2XA(config)# ip dhcp server ?
<cr>
SM12DP2XA(config)# ip dhcp server
SM12DP2XA(config)# end
SM12DP2XA# show ip dhcp server
DHCP server is globally enabled.
All VLANs are disabled.
SM12DP2XA#
```

Command: DHCP Per Port VLAN

Syntax: **ip dhcp server per**-port [vlan { <pertPortVLAN> }]

Description: The DHCP Per Port VLAN function lets you have an IP address from a DHCP pool on a switch be statically assigned to a switchport, such that whichever device plugs into the switchport it will always be assigned that specific IP address. The IP address is configured in the interface config settings. Note that this is binding an IP address to an interface, not to a MAC address, which is the classic binding technique found on most switches. 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. (Added at FW VB7.20.0140.) See the IP command on page 48 for more information.

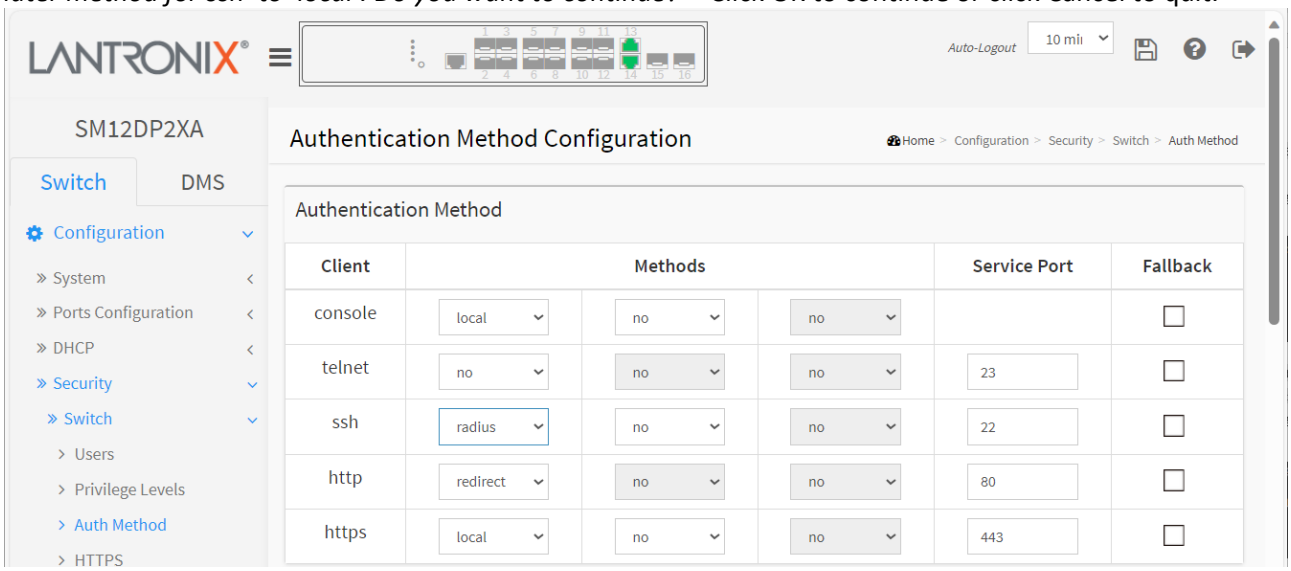
Example:

```
SM12DP2XA(config)# ip dhcp server ?
   per-port    Enable DHCP server per port
SM12DP2XA(config)# ip dhcp server per-port ?
   vlan    DHCP server per port VLAN
   <cr>
SM12DP2XA(config)# ip dhcp server per-port vlan ?
   <vlan_id>    Set DHCP server per port VLAN
SM12DP2XA(config)# ip dhcp server per-port vlan 100 ?
   <cr>
SM12DP2XA(config)# ip dhcp server per-port vlan 100
SM12DP2XA(config)# do show ip dhcp server

DHCP server is globally enabled.
  All VLANs are disabled.
  DHCP server per port is enabled.

SM12DP2XA(config)#
```

Appendix B. Secure File Transfer (SFTP) Set-Up

Switch Settings : RADIUS Authentication Using SSH Putty Port 22

***Warning**: When setting first method for 'ssh' to other than 'local', you may lose connectivity unless you set a later method for'ssh' to 'local'. Do you want to continue?* Click OK to continue or click Cancel to quit.

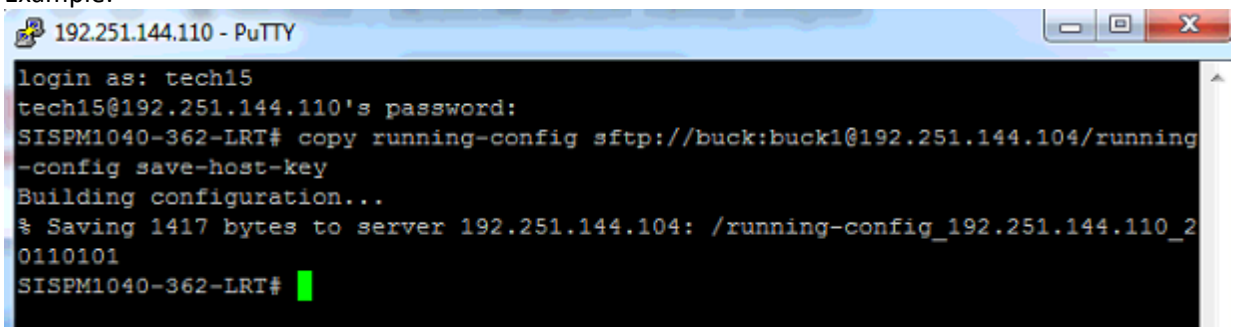


CLI Command:

```
copy running-config sftp://buck:buck1@192.251.144.104/running-config save-host-key
```

Description: Transfer running-config from switch to SolarWinds, using SFTP protocol.

Example:



CLI Command: `copy startup-config sftp://buck:buck1@192.251.144.104/startup-config-radius save-host-key`
Description: Transfer startup-config from switch to SolarWinds, using SFTP protocol.
Example:

```
SISPM1040-362-LRT# copy startup-config sftp://buck:buck1@192.251.144.104/startup
-config-radius save-host-key
% Saving 1239 bytes to server 192.251.144.104: /startup-config-radius_192.251.14
4.110_20110101
SISPM1040-362-LRT#
```

CLI Command: `copy sftp://tech15:15tech@192.251.144.104/startup-config_192.251.144.110_20110101 startup-config save-host-key`
Description: Transfer startup-config from SolarWinds to switch, using SFTP protocol
Example:

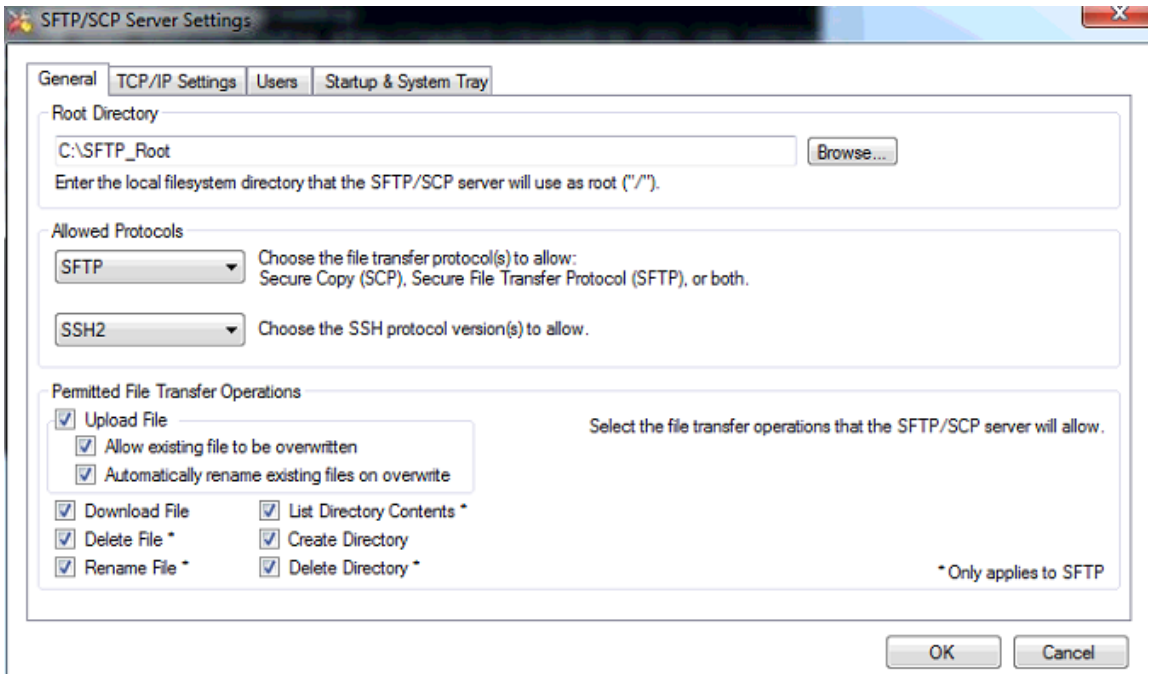
```
SISPM1040-362-LRT# copy sftp://tech15:15tech@192.251.144.104/startup-config_192.
251.144.110_20110101 startup-config save-host-key
% Loading /startup-config_192.251.144.110_20110101 from SFTP server 192.251.144.
104
% Saving 1004 bytes to flash:startup-config
SISPM1040-362-LRT#
```

CLI Command: `copy running-config sftp://tech15:15tech@192.251.144.104/running-config save-host-key`
Description: Transfer running-config from SolarWinds to switch using SFTP protocol
Example:

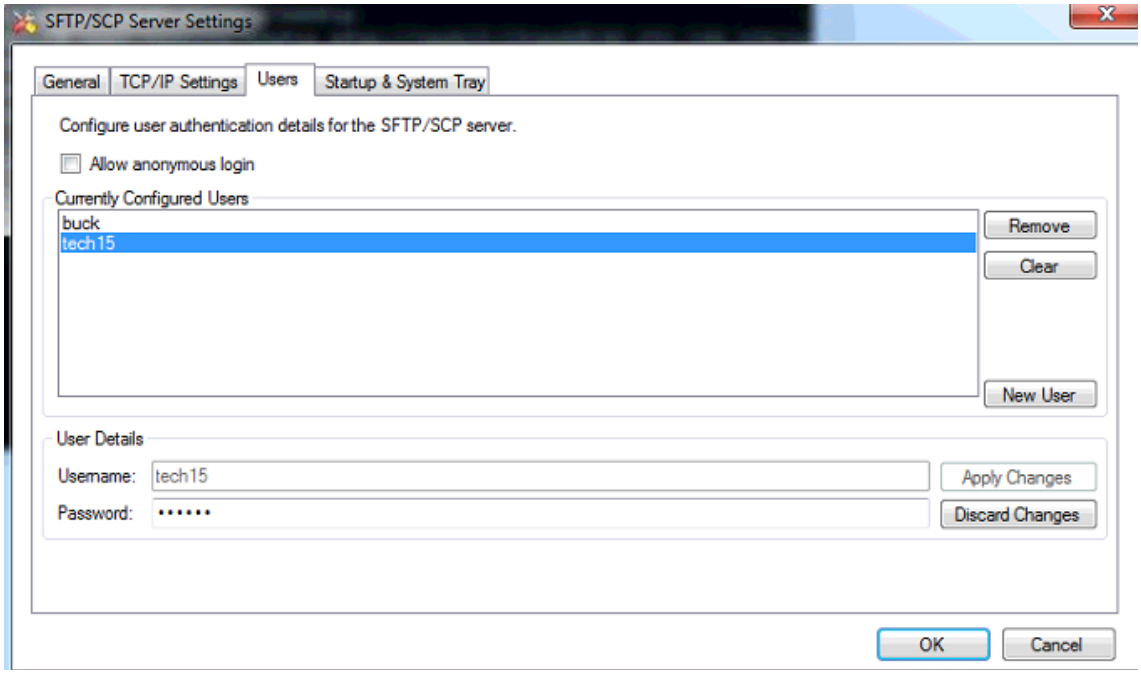
```
SISPM1040-362-LRT# copy running-config sftp://tech15:15tech@192.251.144.104/runn
ing-config save-host-key
Building configuration...
% Saving 1417 bytes to server 192.251.144.104: /running-config_192.251.144.110_2
0110101
SISPM1040-362-LRT#
```

Solar Winds Settings

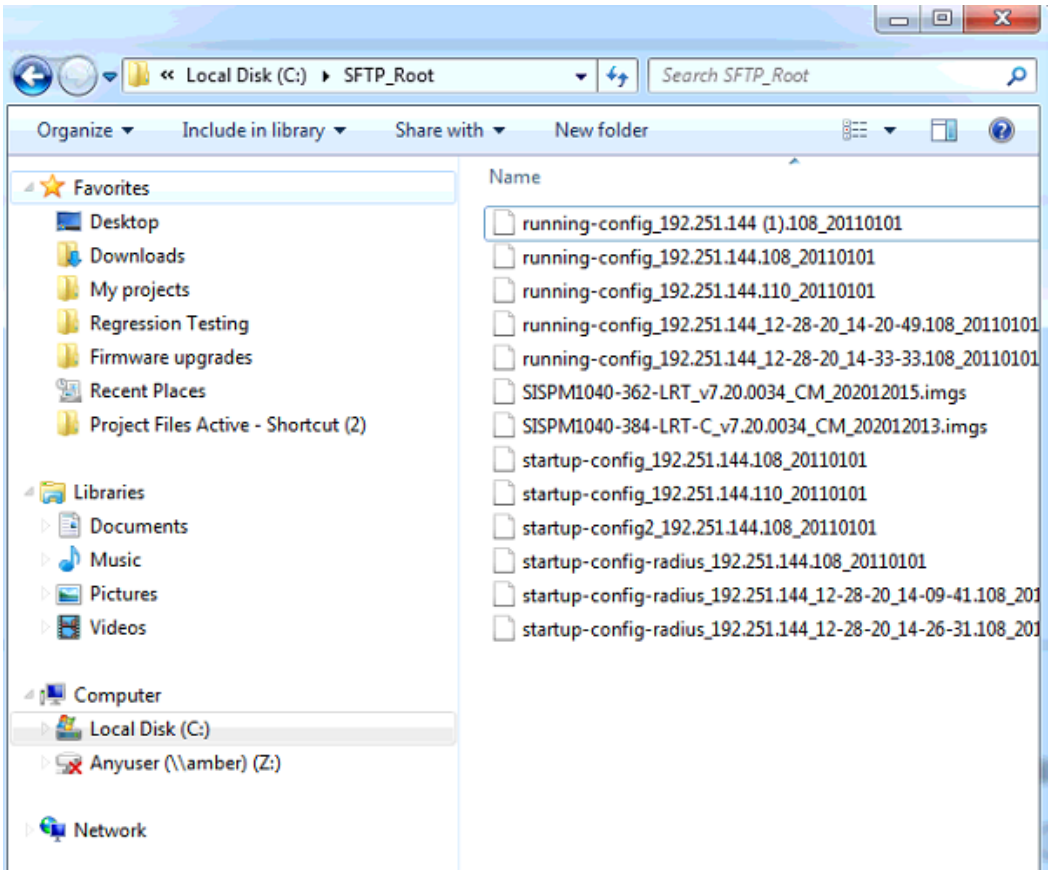
General tab



Users tab



Windows Explorer



Lantronix Corporate Headquarters

48 Discovery, Suite 250
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support

Online: https://www.lantronix.com/technical-support/

Sales Offices

For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about/contact