



Focal Point™ 2.1 Management Software
&
CPSMM100 Firmware
Manual

Manual
33293 Rev B

Table of Contents

Section I:	1
Introduction	1
About this manual	2
CPSMM100-xxx firmware overview	4
Focal Point management software overview	5
Simple Network Management Protocol (SNMP) overview	6
Section II:	9
Focal Point Management Software.....	9
Hardware setup.....	10
Focal Point software installation	11
Focal Point main window pull-down menus.....	13
Focal Point management software overview	19
Focal Point software web-based management	31
CPSMM100 firmware upgrades	36
Section III	39
Command-Line Interface (CLI).....	39
DB-9 serial port CLA access	40
RJ-45 Ethernet port CLA access	45
Network security.....	48
Redundant base-management module (MMU) configuration.....	57
Command-line interface reference information	59
Section IV:.....	65
Troubleshooting & Cable Specifications.....	65
Troubleshooting problem and corrective action table.....	66
Cable specifications	69
Section V:.....	71
Contact Us & Warranty	71
Contact us.....	72
Warranty.....	73
Index.....	75

Intentionally Blank

Trademark and copyright information

Trademark

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

Copyright restrictions

© 2006 Transition Networks. All rights reserved. No part of this work may be reproduced, translated, or used in any form or by any means—graphic, electronic, or mechanical—without written permission from Transition Networks.

Printed in the U.S.A.

Intentionally Blank

Section I: Introduction

In this section These are the topics:

Topic	See Page
About this manual	2
CPSMM100-xxx firmware overview	4
Focal Point management software overview	5
Simple Network Management Protocol (SNMP)	6

About this manual

Point System chassis management

This manual explains how to set up (*via a computer interface*) Transition Networks' (TN) Focal Point management software and the CPSMM100 firmware used to monitor and manage one or more Point System chassis populated with Transition Networks' media converters. The management system is comprised of the following:

- Focal Point management software
 - CPSMM100-xxx management module (MMU) and firmware
 - Management
 - SNMP management protocol
 - Point System chassis containing various Transition Networks' cards.
-

Point system chassis

The following is a list of Point System products:

- Point System chassis (*single, dual, 8, 13, 18 or 19 slot*)
- Point System slide-in-module media converters
- Point System management modules
- Focal Point 2.x management software (*see website for current version*)
- Point System power supply modules
- Point System accessories

Visit **www.transition.com** for complete details on Point System chassis products.



Figure 1: 19-Slot Point System™ Chassis

Continued on next page

About this manual, continued

How this manual is constructed

This manual is divided into five sections, each with a beginning table of contents. The manual also has the following:

- Index
 - Appendix A: Command-Line Interface Commands (*separate document*)
 - Appendix B: Command-Line Interface Messages (*separate document*)
-

Focal Point new feature for version 2.1

Get/Set MIB values.

The administrator can retrieve and modify MIB variable values of a module, using the command-line interface (CLI). To do this, the administrator must know the ‘serial number’ of the chassis and the ‘slot number’ of the module.

CPSMM100-xxx firmware overview

Firmware location The CPSMM100-xxx firmware is embedded in Transition Networks management modules.

Management module and firmware P/Ns The following table shows the firmware in specific Transition Networks' management modules:

Management Module	Firmware P/N
CPSMM-120 Single-Slot	CPSMM100-120
CPSMM-200 Dual-Slot	CPSMM100-200
SMACF10xx-20x media converter's management module	CPSMM100-400

What is in each firmware version? Each version of the CPSMM100-xxx firmware contains:

- Transition Networks' Point System Command Line Interface (CLI)
- An embedded Telnet server
- An embedded Web server
- An SNMP (*Simple Network Management Protocol*) agent

Focal Point management software overview

Focal Point description

Transition Networks' Focal Point management software (*an implementation of SNMP*) installs on a networked computer to provide a graphical user interface (GUI) to monitor the Point System chassis and its modules.

Management methods

In a network that includes one or more management module(s), the administrator can monitor and manage the Point System chassis and its individual media converters via:

- A CLI at an attached terminal
 - A CLI at a remote Telnet connection
 - A remote Web browser
 - SNMP software, such as Transition Networks' Focal Point management software, installed on a remote Network Management Station (NMS)
-

Features

The software includes these features:

- Graphical user interface (GUI)
 - Status monitoring
 - Enable/disable converter features
 - Universal trap viewer/receiver
 - One-click telnet
 - Upgrade tool
 - Live chat with Transition Networks' tech-support personnel
 - Direct links to product literature
 - Transition agent discovery capability
-

Simple Network Management Protocol (SNMP) overview

SNMP definition SNMP is a request-response protocol that defines network communication between a managed device and a network management station (NMS).

How is SNMP managed? SNMP is anything but simple. The good news is that the details of SNMP are managed very well by Transition Networks CPSMM100-xxx firmware and the Focal Point management software. A more lengthy and detailed explanation of SNMP can be found at: www.transition.com/pshelp/snmp.html

SNMP terms The following terms will help enable a better understanding of SNMP:

Managed Device:
A managed device is a hardware unit with embedded firmware connected to a network with SNMP management capabilities.
An example of a managed device is Transition Networks' 19-slot chassis with an installed management module and one or more installed card media converters shown in Figure 1 on the "About this manual" page.

Network Management Station (NMS):
An NMS is a high-end workstation connected to the network like other managed device.

Management Information Base (MIB):
The MIB is a set of variables used to monitor and control a managed device.

Managed Object or MIB variable:
The individual variables that make up the MIB are called managed objects or MIB variables. These variables are the individual features of the managed device. The administrator can use these variables to monitor and configure the managed device. For example, a card from Transition Networks can have up to 20 or more managed objects (*MIB variables*) associated with it. Some examples are the following:

- Power ON/OFF the card
- Enable the AutoCross feature
- Display activity on the fiber link, etc.

Continued on next page

Simple Network Management Protocol (SNMP) overview, continued

**SNMP
operations**

SNMP has four defined operations. These operations allow the administrator to monitor and control the managed device from a remote location. The four operations are the following:

GET and GET-NEXT:

To monitor (*or read*) the managed device, the administrator initiates, through the user interface to the network management software on the NMS, the GET and GET-NEXT operations on selected called instances of managed objects (*variables*) in the MIB of the managed device.

SET:

To control (*or write*) the managed device, the administrator initiates, through the user interface to the network management software on the NMS, the SET operation on selected instances of managed objects in the managed device's MIB.

TRAP:

To alert the administrator about instances of MIB-defined asynchronous events on the managed device, the SNMP agent initiates the TRAP operation through the user interface to the network management application on the NMS.

Intentionally Blank

Section II:

Focal Point Management Software

Introduction Transition Networks' Focal Point management software is a graphical user interface (GUI) that allows the administrator to monitor and control a Point System chassis and its modules from a remote NMS.

In this section These are the topics:

Topic	See Page
Hardware setup	10
Focal Point software installation	11
Focal Point main window pull-down menus	13
Focal Point management software overview	19
Focal Point software web-based management	31
CPSMM100 firmware updates	36

Hardware setup

Point System chassis hardware setup

The hardware setup begins with one or more Transition Networks' management modules (*CPSMM-200* or *CPSMM-120*) installed in one or more Transition Networks' Point System™ chassis:

- CPSMC0200-2xx 2-slot chassis
- CPSMC0800-100 8-slot chassis
- CPSMC13xx-100 13-slot chassis
- CPSMC18xx-xxx 18-slot chassis
- CPSMC19xx-100 19-slot chassis

Next, the management module must be connected via an Ethernet port to a TCP/IP network that is accessible via IP from the NMS. See Figure 2.

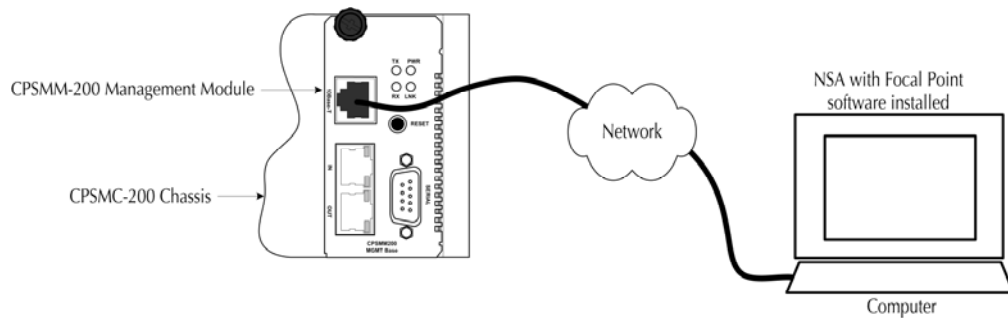


Figure 2: CPSMM-200 Management by NAS with Focal Point Software

Focal Point software installation

Introduction

The following procedures show how to install the Focal Point software on a remote UNIX or Windows NMS.

UNIX OS installation

To install the Focal Point software on a UNIX NMS, do the following:

Step	Action
1.	Insert the installation CD into the computer's CD drive.
2.	Run the installation script: "fp.sh" on the enclosed CD in the directory <code>\fp2\TransitionNetworks\unix\</code>
3.	Follow the instructions on the display to complete the installation.

Windows OS installation

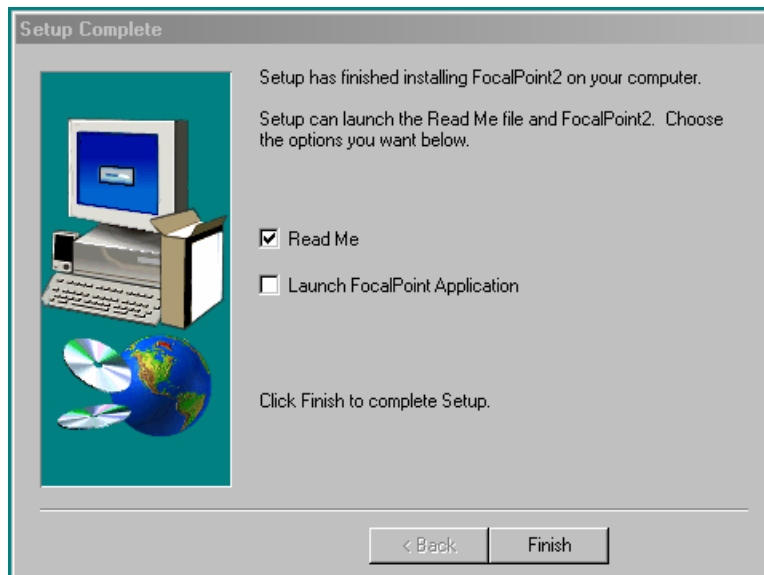
To install the Focal Point software on a Windows NMS, do the following:

Step	Action
1.	<ul style="list-style-type: none"> Insert the installation CD into the computer's CD drive and the "Welcome" dialog box will appear. Or run the executable file: setup.exe on the CD in the directory <code>\TransitionNetworks\win\</code> and the "Welcome" dialog box will appear.
2.	Click the NEXT button and the "Choose Setup Type" dialog box will appear.
3.	Highlight the "setup type" for your particular operating system: <ul style="list-style-type: none"> Cisco Works -- Install the software on a system with CiscoWorks present. HP OpenView -- Install the software on a system with HP OpenView present. Stand Alone -- Install the software on a system with Windows 95/98/2000/NT or XP software present.
4.	Click the NEXT button and the "Choose Destination Folder" dialog box will appear. Use this window to select where to install the software.
5.	Click the NEXT button to install the software in the default folder; or create or select another folder from the list of existing folders.

Continued on next page

Focal Point software installation, continued***Windows OS installation (continued)***

Step	Action
6.	Click the NEXT button and the “Start Copying Files” dialog box will appear.
7.	<ul style="list-style-type: none"> • Click the BACK button to review or change any settings. • Click the NEXT button to start copying the program files.
8.	When the “Setup Complete” dialog box appears, click the FINISH button to complete the setup process. See Figure 3.

**Figure 3: Setup Complete Screen**

9.	If an “Information” dialog box appears, click the NEXT button to complete the installation.
----	---

Focal Point main window pull-down menus

Focal Point main window

Click the Focal Point icon at the remote NMS and a Focal Point window will appear as shown in Figure 4. The Focal Point main window has four pull-down menus: File, View, Tools, and Help. The following is an explanation of the selections on each pull-down menu.

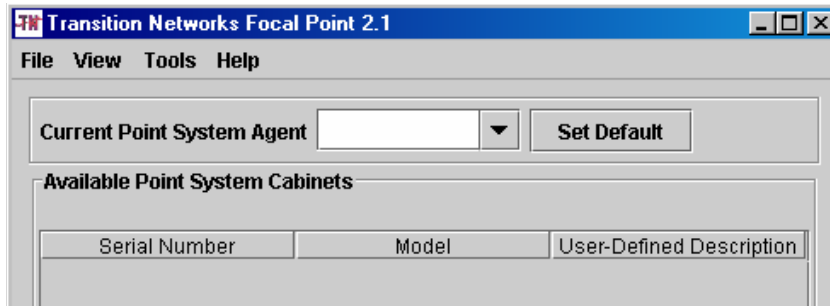


Figure 4: Focal Point Main Window

File pull-down menu

On the 'File' pull-down menu Exit is the only item. Select Exit to close the Focal Point main window and the CLI. See Figure 5.

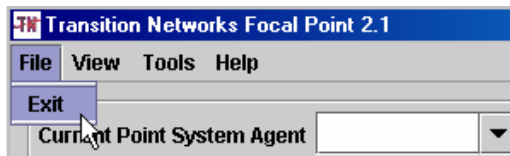


Figure 5: File Pull-Down Menu Item Exit

Continued on next page

Focal Point main window pull-down menus, continued

View pull-down menu The ‘View’ pull-down menu items are Refresh, Import Logo Image, and Remove Log Image (*grayed out*). See Figure 6.

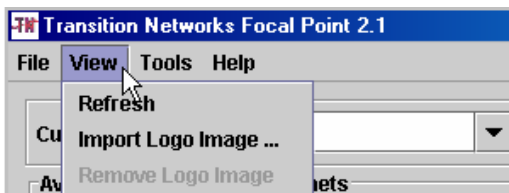


Figure 6: View Pull-Down Menu

The following is an explanation of the items on the “View” pull-down menu.

Refresh: Refreshes the Focal Point main window. Select Refresh (*or press the ENTER key*) after entering an IP address of the cabinet to be monitored.

Import Logo Image: Imports a company logo (*JPG or GIF format*) and adds it to the “Focal Point” main window and to the “Cabinet View” dialog box. This function allows personalizing the software displays.

Remove Logo Image: Removes the imported logo image from both the “Focal Point main window and to the “Cabinet View” dialog box. (*This item is grayed out until a logo is imported.*)

Tools pull-down menu

The ‘Tools’ pull-down menu items are Trap Server, Trap Viewer, Application Settings, Node Configuration, Collect Server Configuration, Text Editor, and Discover Transition Agent. See Figure 7.

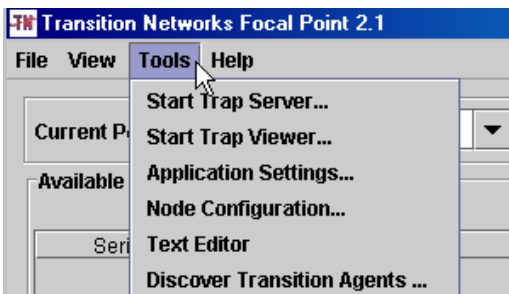



Figure 7: Tools Pull-Down Menu

Continued on next page

Focal Point main window pull-down menus, continued

Tools pull-down menu (continued)

The following is an explanation of the items on the “Tools” pull-down menu.

Trap Server: Select “Trap Server...” to open the Trap Server application and a Transition Networks’ icon  will appear in the bottom-right corner of the computer screen to indicate that the Trap Server application is running.

The Trap Server application collects and displays SNMP traps. It consists of a receiver component that listens for traps, and a viewer that displays them in a readable format.

Trap Viewer: Opens the “SNMP Trap Viewer” window. The window lists the traps specific to Transition Networks’ Point System agent. See Figure 8.

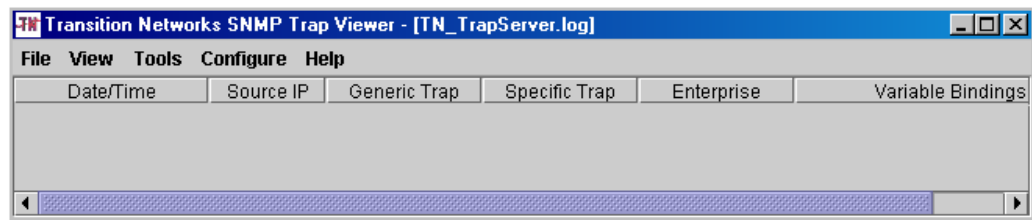


Figure 8: Trap Viewer Window

Select [Help] and then [Contents] on the Trap Viewer window for information on the Trap Viewer application. The help-screen files are current to the date of the product CD. The most current files are at www.transition.com/pshelp/traps.html

Application Settings: Allows applying the following changes to the Focal Point software: security level, polling rate (*in seconds*), and configuration log file size (*in kilobytes*). These changes are logged to the SNMP agent. See Figure 9.

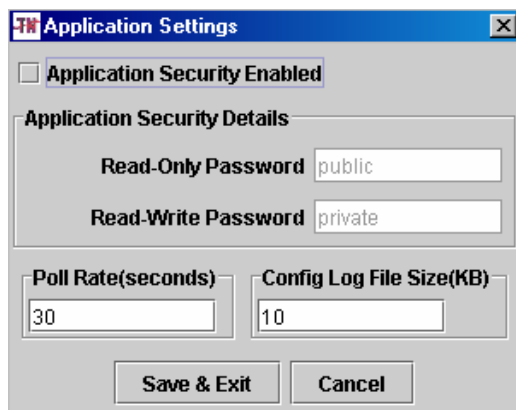


Figure 9: Application Settings Dialog Box

Continued on next page

Focal Point main window pull-down menus, continued***Tools pull-down menu (continued)***

Node Configuration: Allows establishing the basic application settings for each node (*i.e.*, IP address) and the default setting for all nodes. This includes the password, time-out duration, number of retries, port and description. See Figure 10.

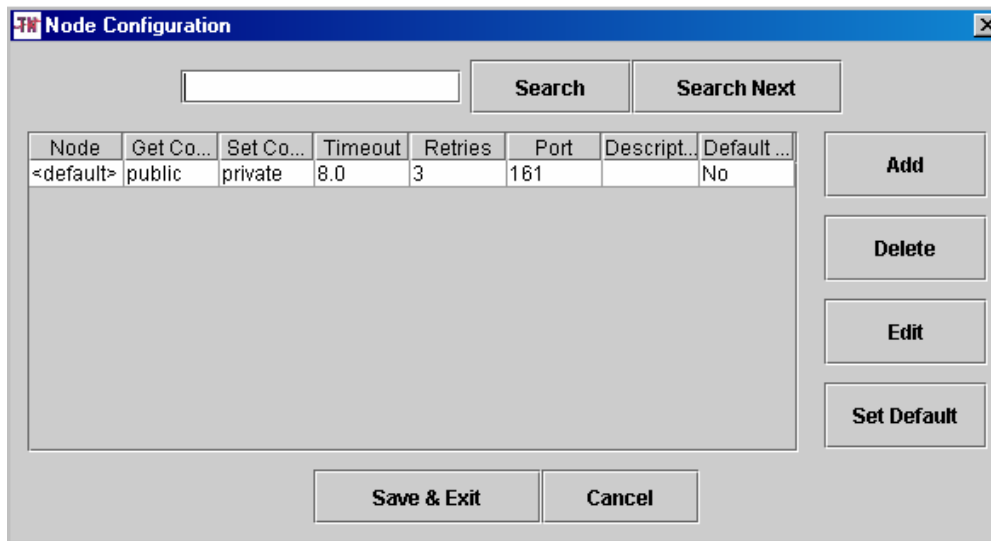


Figure 10: Node Configuration Dialog Box

Collector Server Configuration: The collector application uses a database as a data repository to store all records received from a Transition Networks agent running an SMACF100 device. The administrator must first install both the database and the tables used by the collector. Any database can be used since the application runs independent of the database type.

For a detailed description of the Collector Server, see the document “Collector DB.doc” in the directory: ...\\Program Files\\Transition\\Focal Point2\\doc\\. This file installs on the hard drive during the Focal Point software installation.

Text Editor: Opens a simple text editor. Text can be entered via the keyboard. It can be copied from one application (*using the Ctrl-C keys*), pasted to another application (*using the Ctrl-V keys*), and then saved by selecting File\\Save from the text-editor menu bar.

Only one such file can be saved at a time, so there is no need to name the file. When the Focal Point software closes, the information is saved. The information can be retrieved when Focal Point re-opens.

Continued on next page

Focal Point main window pull-down menus, continued***Tools pull-down menu (continued)***

Discover Transition Agents: Allows the administrator to search for available IP addresses. This application “pings” each address in the entered range. If a response is received, then the Host IP address is valid.

To search a range of IP addresses, do the following:

Step	Action
1.	Select “Discover Transition Agents” from the “Tools” pull-down menu and a Discover Transition Agents dialog box will appear. See Figure 11.
2.	Enter a range of IP addresses in the [From IP] and the [To IP] text fields, as shown in Figure 11.
3.	Click the START DISCOVERY button and the application will list the available IP addresses in that range, as shown in Figure 11. <i>(To stop the search at any time, click the STOP DISCOVERY button to stop the search.)</i>
4.	Click the SAVE button to save the results of the search.
5.	Click the CLOSE button to close the “Discovering Transition Agents” dialog box.

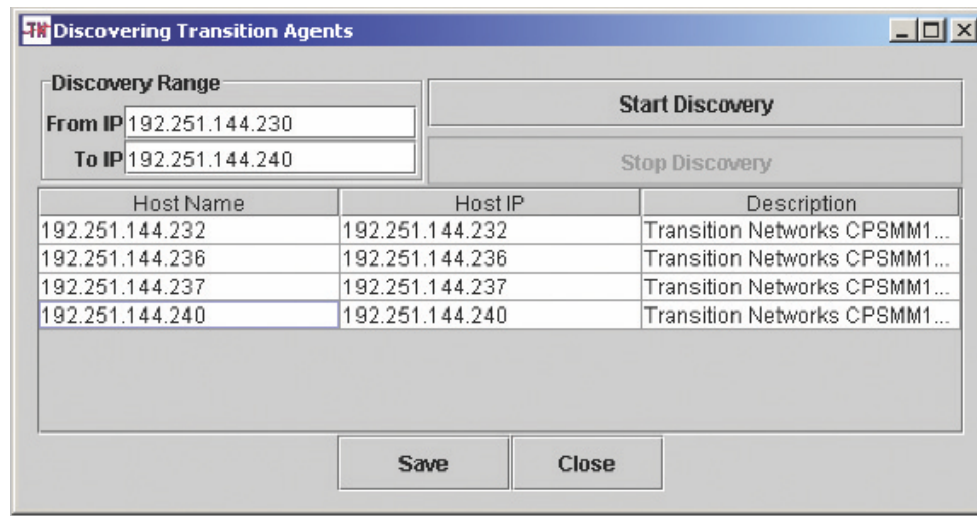


Figure 11: Discovering Transition Agents Dialog Box

Continued on next page

Focal Point main window pull-down menus, continued**Help pull-down menu**

Main window 'Help' pull-down menu items are Contents and About. See Figure 12.

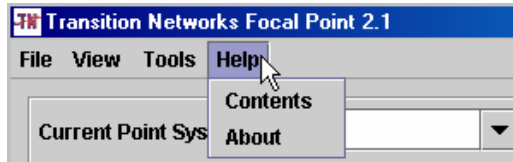


Figure 12: Help Pull-Down Menu

The following is an explanation of the items on the 'Help' pull-down menu.

Contents: Opens the Web browser to Focal Point help pages. These help pages were installed onto the computer's hard drive when the application was installed. The files are current to the date the CD was produced. For the most current Help files go to www.transition.com/pshelp

About: Lists the Focal Point software version, copyright, and contact information for Transition Networks.

Focal Point management software overview

Accessing a cabinet via Focal Point

To access a Transition Networks' CPSMC cabinet on the network, do the following:

Step	Action
1.	Enter an IP address in the [Current Point System Agent] text box as shown in Figure 13.
2.	Press ENTER and the CPSMC cabinet model number will appear under 'Model' as shown in Figure 13.

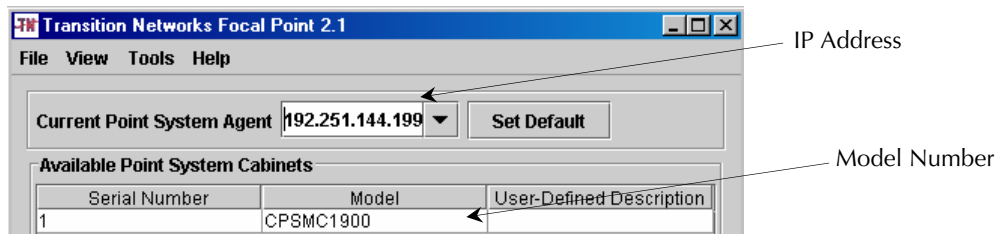


Figure 13: Enter Current Point System Agent IP address

Viewing IP address history

Focal Point also saves all previously entered IP addresses. Click the [Current Point System Agent] DOWN arrow to display an IP address history. See Figure 14.

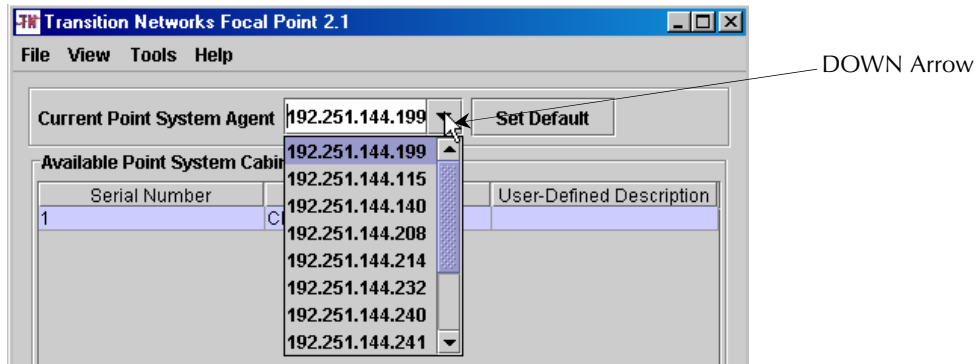


Figure 14: IP Address History

Continued on next page

Focal Point management software overview, continued

Set default button

Click the SET DEFAULT button shown in Figure 15 to keep the current IP address as the default whenever the Focal Point management software opens.

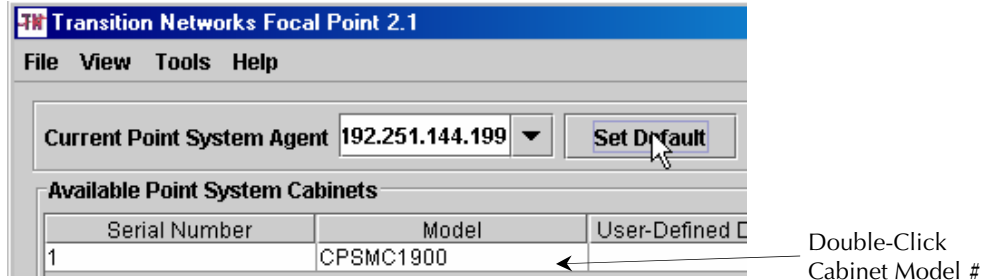


Figure 15: Set Default Button

Available point system cabinets

Double-click the [cabinet model number], shown in Figure 15 above, to launch the Point System chassis “Cabinet View” dialog box shown in Figure 16.

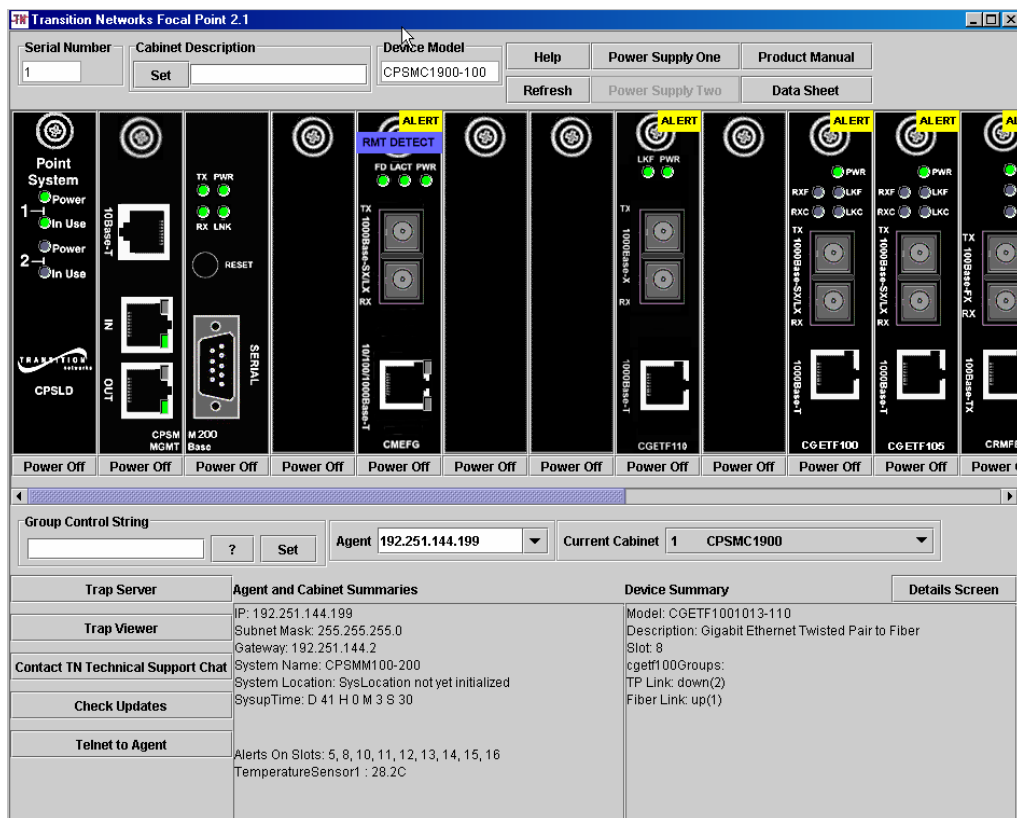


Figure 16: Cabinet View Dialog Box (shows all installed cards)

Continued on next page

Focal Point management software overview, continued**Cabinet view,
graphical card**

The main feature of the “Cabinet View” dialog box is the graphical cards. The modules are represented by white-on-black line drawings that represent all modules in the Point System chassis. The modules that appear include:

- Power Supplies
- Management Modules
- Media Converters

The following describes the remaining elements of the cabinet view dialog box.

**Cabinet view,
purple slide**

The purple slide-bar, in the center of the cabinet view dialog box, allows viewing the entire graphical chassis by moving the slide to the module of choice. See Figure 17.



Figure 17: Purple Slide

**Cabinet view,
module alerts**

A yellow [Alert] tag, on the graphical cards shown in Figure 18, indicates that particular module is in hardware mode and cannot be configured via the Focal Point software. See the product manual for the any specific card for more information.



Figure 18: Module Alert

Continued on next page

Focal Point management software overview, continued**Cabinet view,
agent/cabinet
summaries field**

The [Agent and Cabinet Summaries] field (*in the bottom-center of the cabinet view dialog box*) lists the details of the agent and the cabinet. See Figure 19.

Agent and Cabinet Summaries
IP: 192.251.144.199
Subnet Mask: 255.255.255.0
Gateway: 192.251.144.2
System Name: CPSMM100-200
System Location: SysLocation not yet initialized
SysupTime: D 28 H 22 M 31 S 41
Alerts On Slots: 5, 8, 10, 11, 12, 13, 14, 15, 16
TemperatureSensor1 : 27.3C

Figure 19: Agent and Cabinet Summaries

**Cabinet view,
device
summary field**

Single-click any of the graphical cards to show that module's details in the [Device Summary] field (*in the bottom right side of the cabinet view dialog box*). Focal Point will display the details of a selected management module (*CPSMM-120, CPSMM-200, or CPSMM-210*) in the [Device Summary] field. See Figure 20.

Device Summary
Model: CPSLD100-100
Description: Power Supply Indicator Card
Slot: 1
Power Supply 1 Power: On(1)
Power Supply 1 In Use: yes(1)
Power Supply 2 Power: unknown(2)
Power Supply 2 In Use: no(2)

Figure 20: Selected Device Summary Information

Continued on next page

Focal Point management software overview, continued**Cabinet view, details screen button**

Click the DETAILS SCREEN button to open the “Details” dialog box for the selected module. See Figure 21.

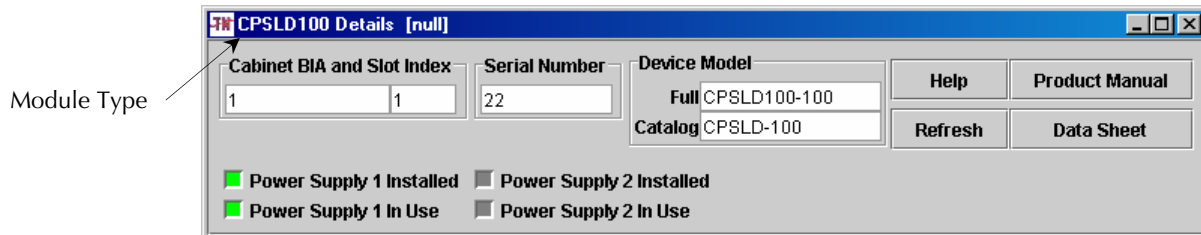


Figure 21: Module Details Summary Dialog Box

Cabinet view, serial number and device model fields

These serial number and device model fields automatically populate with the device serial number and model number of the chassis when the cabinet view dialog box is launched. See Figure 22.

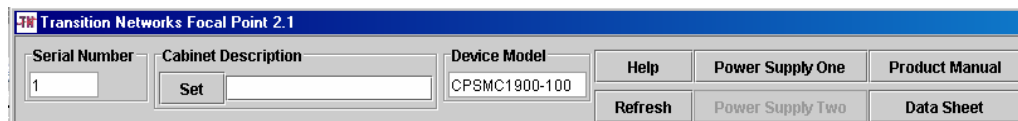


Figure 22: Cabinet View Dialog box

A description of the remaining fields and bottoms shown in Figure 22 are as follows:

Cabinet Description: Enter a user-defined description of the chassis or other device displayed in the “Cabinet View” dialog box. Click the SET button to save the description.

HELP button: Click the HELP button to display web-based links to an integrated set of help files that present instructions for using Focal Point software. You can view and print the help files from any standard HTML browser.

Help-screen files are only current to the date of the CD production. The most current files are at www.transition.com/pshelp

REFRESH button: Click the REFRESH button to update all fields in the “Cabinet View” dialog box.

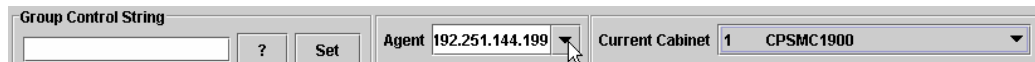
POWER SUPPLY ONE and TWO buttons: Click either button to display the details of the power supply. This information is listed in a separate dialog box.

PRODUCT MANUAL and DATA SHEET buttons: Click either button to open a web browser window that displays the product manual or the data sheet of the cabinet (*Point System chassis or other device*) shown in the “Cabinet View” dialog box.

Continued on next page

Focal Point management software overview, continued**Cabinet view dialog box (continued)****Cabinet view, group control string, agent, current cabinet**

Group Control String text field: The primary function of the group control string text field shown in Figure 23 is to allow the grouping of two or more identical media converters so that a single configuration change will apply to all devices in the group. Click the [?] button to show additional functions of the group control string feature.

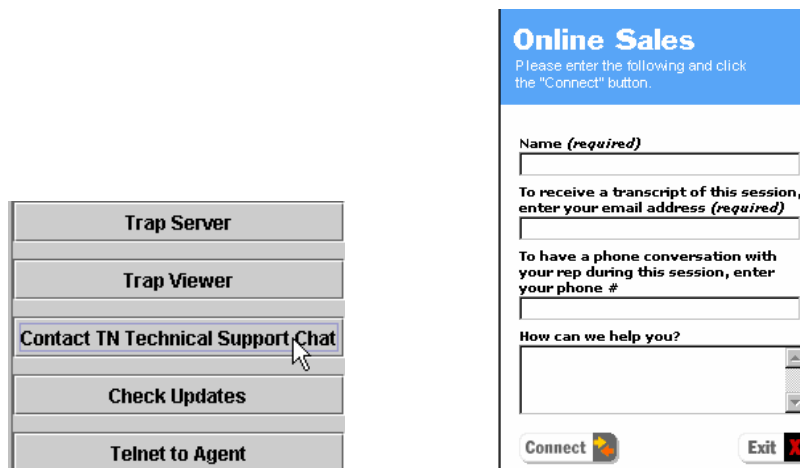
**Figure 23: Group Control String, Agent, and Current Cabinet**

Agent: Enter an IP address in the [Agent] field shown in Figure 23. Press the ENTER key to view the details of a new agent. Focal Point also saves all previously entered IP addresses. Click the DOWN arrow to see previously entered IP addresses. This feature allows quick switching to a new agent without opening a new window.

Current Cabinet drop-down box: The [Current Cabinet] drop-down box shown in Figure 23 is automatically populated with the cabinet (*Point System chassis or other device*) associated with the current agent. Additional cabinets within the same agent can be displayed by clicking the DOWN ARROW to select a new cabinet. This feature allows for quick switching to a different cabinet without opening a new window.

Cabinet view, contact TN tech service chat button

Click the CONTACT TN TECHNICAL SERVICE CHAT button to open a Web browser window for a chat session with a Transition Networks service technician. See Figure 24. Representatives are available 24 hours a day.

**Figure 24: Contact TN Tech Service Chat Button and Technical Session Screen***Continued on next page*

Focal Point management software overview, continued

**Cabinet view,
update button**

To get the latest version of the software, click the CHECK UPDATES button to open a browser window to Transition Networks’ website. See Figure 25. Contact Technical Service for additional information or assistance.

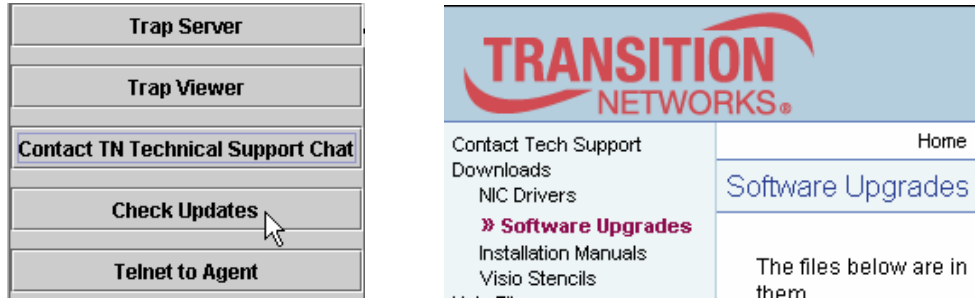


Figure 25: Check Updates Button and Upgrade Screen

**Cabinet view,
telnet to agent
button**

Click the TELNET TO AGENT button to open a Telnet session, which will bring up the password screen, shown in Figure 26.



Figure 26: Telnet to Agent Button and Telnet Session Log In Screen

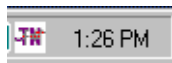
Continued on next page

Focal Point management software overview, continued**Trap server application**

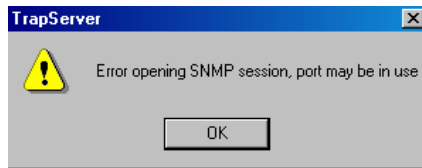
Transition Networks' Trap Server application collects and displays SNMP traps. It consists of a receiver that listens for traps, and a viewer that displays them in a readable format.

Cabinet view, trap server button

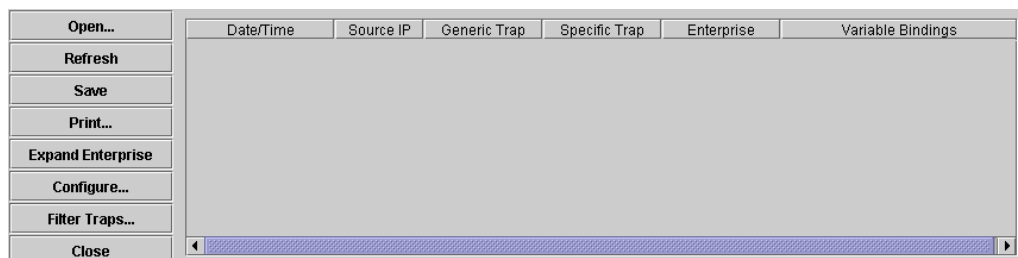
Click the TRAP SERVER button one time to launch Transition Networks Trap Server application. A Transition Networks (TN) icon will appear at the bottom-right corner of the screen, indicating that the Trap Server application is running. See Figure 27.

**Figure 27: TN Trap Server Application Icon**

Note: If you click the TRAP SERVER button after the application launches, the following error message will appear, shown in Figure 28.

**Figure 28: Trap Server Error Message****Cabinet view, trap viewer button**

Click the TRAP VIEWER button to display the trap viewer in the “Cabinet View” dialog box. See Figure 29.

**Figure 29: Trap Viewer**

Note the following on the trap viewer:

- The Trap Viewer window replaces the Agent/Cabinet and Device Summary fields.
- The buttons on the left are replaced with the Trap Viewer function buttons.
- Click the CLOSE button to return to the previous fields.

Continued on next page

Focal Point management software overview, continued

Trap viewer help files

To view the ‘Help files’ for the trap viewer application, do the following:


Step	Action
1.	Left click the Transition Network trap server icon  on the bottom-right corner of the screen to bring up the Tape Server menu shown in Figure 30.



Figure 30: Trap Server Menu

2.	Select item “Trap Viewer” to launch the Trap Viewer window shown in Figure 31.
3.	On the “Trap Viewer” window select [Help] [Contents] as shown in Figure 31, to launch the trap-server help screen.

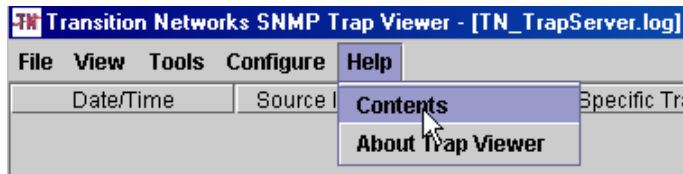


Figure 31: Accessing Trap Viewer Help Files

Note: Help-screen files are only current to the date of the CD production. The most current files can be found at www.transition.com/pshelp/traps.html

Continued on next page

*Focal Point management software overview, continued***Device details dialog box**

From the “Cabinet View” dialog box, double-click any graphical card to open the “Device Details” dialog box for that module as shown in Figure 32.

CGETF100 Details

Cabinet BIA and Slot Index: 1 8 Serial Number: 1 Device Model: Full CGETF1001013-110
 Catalog: CGETF1013-110 Help Product Manual
 Refresh Data Sheet

Copper Connector: RJ-45 - Unshielded Twisted Pair Twisted Pair Link
 Fiber Link
Fiber Connector: SC - Multimode Fiber (SX), Soldered On Fault
 Clock Master

Twisted Pair Length: Less than 50 meters

Device Enabled: Enabled Disable **Fiber Auto Negotiate**: Enabled Enable
Link Pass Through: Enabled Disable **Full Duplex**: Enabled Disable

Remote Fault Detect: Enabled Enable Pause Type: asymTX

Group Management **Fiber DMI**

Click on the button next to the respective feature you wish to manage above. Changes will take affect immediately and will be visible in this application at the next polling interval.

If you would like to apply changes to many devices at once, read the configuration management screen by clicking the Help button below.

Help

cgetf100Groups
 Help Apply

Figure 32: Card Details Dialog Box

Note: The “Device Details” dialog box will have a different format for different module types; however, the functions described are generic to all.

Continued on next page

Focal Point management software overview, continued**Device details dialog box, buttons**

HELP button: (At the top-right of the “Device Details” dialog box) click to display web-based information on the device featured in the “Device Details” dialog box.

REFRESH button: To make changes simply enter the new information into the text field (or select a check box) and click the REFRESH or APPLY button (depending upon the type of “Device Details” dialog box).

Note: Changes made in the “Details” dialog box are saved in non-volatile memory of the card, so the modified configuration follows the card when moved from one slot to another.

PRODUCT MANUAL and DATA SHEET buttons: Click either button to view either the Product Manual or the Data Sheet of the device featured in the “Details” dialog box.

Note: Grayed out check and text boxes means those functions are not available.

Device details dialog box, yellow attention notice

A yellow attention tag on the “Details” dialog box, shown in Figure 33, indicates that particular card is in hardware mode and cannot be configured via the Focal Point software. For additional information see the product manual for the selected module.

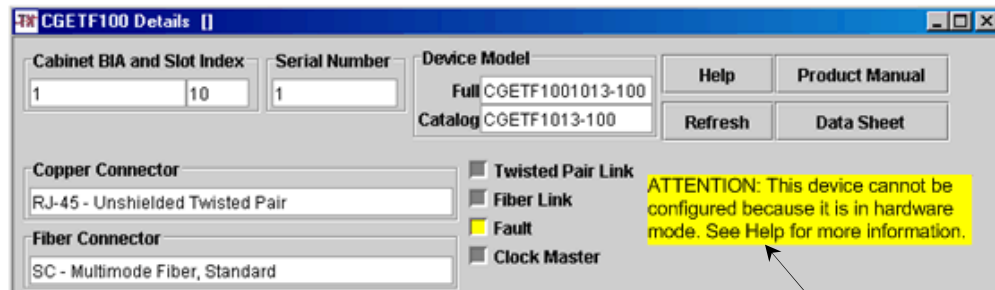


Figure 33: Module Attention Notice (hardware mode)

Yellow Attention Tag

Continued on next page

Focal Point management software overview, continued

Device details dialog box, group management

The group management portion of the “Details” dialog box allows placing devices in groups. The Point System SNMP agent can be used to apply a single configuration change to a group of the same card types. See Figure 34 (*lower part of Device Details dialog box*).

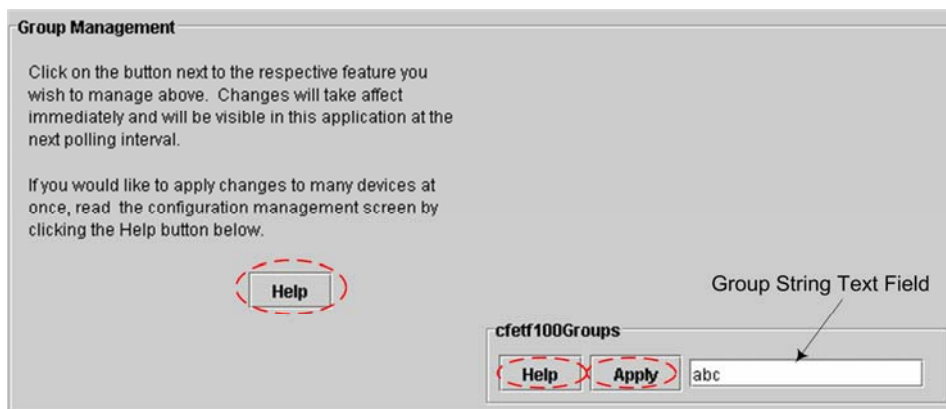


Figure 34: Group Management Portion of the Details Dialog Box

Note: Both HELP buttons show the same information.

HELP button: Click a HELP button shown in Figure 34 to display a web-based help screen that shows detailed instructions for using the group management function—view or print the help screens from any standard HTML browser.

Help-screen files are only current to the date of the CD production. The most current files are found at www.transition.com/pshelp

Group String Text Field: The Group String text field shown in Figure 34 is used to select the previously defined Group strings, or to add new strings by entering a new name into the text field and then clicking the APPLY button.

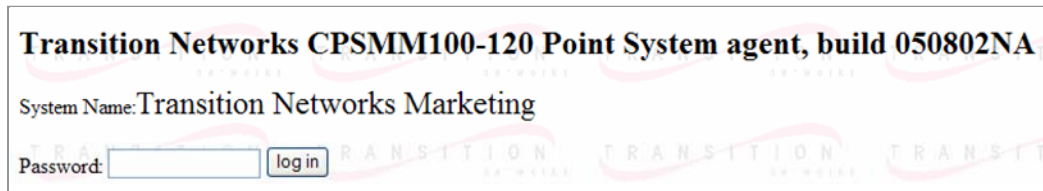
Note: For additional information go to: www.transition.com/pshelp/configmgmt2.html and click the Group Control String link.

Focal Point software web-based management

Introduction Transition Networks' management modules CPSMM-120 and CPSMM-200 install into a Point System chassis. The CPSMM-400 is factory-installed in the SMACF bridge media converter—all contain an embedded HTTP (*Web*) server. This allows monitoring and managing a Point System chassis from a remote location via a standard Web browser.

Accessing Point System Web interface To access the Transition Networks' Point System Web interface, connect to the management module using the appropriate Web browser method. Connection typically is made by entering the IP address or the DNS name of the Point System base management module into the location or the Web browser address field to access the login window.

Log-in screen When the Web connection is made, the login screen will appear. See Figure 35.



Transition Networks CPSMM100-120 Point System agent, build 050802NA

System Name: Transition Networks Marketing

Password:

Figure 35: Log-In Screen

Continued on next page

Focal Point software web-based management, continued**Accessing the agent summary**

To access the agent summary screen, do the following:

Step	Action
1.	Enter a case-sensitive password (<i>default is private</i>) into the password field.
2.	Click the LOG IN button to launch the “Agent Summary” screen as shown in Figure 36.

Transition Networks
Point System Agent Summary
172.16.46.200/Transition Networks Marketing

Cabinets			
	Description	Model	S/N
view	Transition Networks 19-Slot Chassis	CPSMC1900	06421

Group Control String

System uptime (d:h:m:s) : 17:00:57:10

Figure 36: Point System Agent Summary Screen

Agent summary screen elements description

The following describes the elements of the “Point System Agent Summary” screen, Figure 36.

Description field: Enter a user-defined description for the chassis in the accompanying text field and click the APPLY button to save the description.

Group Control String link: The group control string allows displaying only those devices that have been previously added to a group membership. The group membership for each individual device is set in the “Device Details” dialog box.

REFRESH button: Reloads the current web page.

Help Topics link: Opens an integrated set of help screens that provide help for using the embedded HTTP (*Web*) server software. The help screens can be viewed and printed from any standard HTML browser. Help-screen files are current to the date the CD was produced. The most current files are at www.transition.com/pshelp

VIEW button: Shows the “Device Summary” screen for the corresponding chassis. This screen lists all the card devices installed in the chassis.

Continued on next page

Focal Point software web-based management, continued

Device summary screen

From the “Agent Summary” main screen, double-click the VIEW button to show the “Device Summary” screen. This screen displays summary information for each card installed in the chassis. See Figure 37.

Transition Networks 19-Slot Chassis		
Slot Power for cabinet S/N 6421 1: <input checked="" type="checkbox"/> 2: <input checked="" type="checkbox"/> 3: <input checked="" type="checkbox"/> 4: <input checked="" type="checkbox"/> 5: <input checked="" type="checkbox"/> 6: <input checked="" type="checkbox"/> 7: <input checked="" type="checkbox"/> 8: <input checked="" type="checkbox"/> 9: <input checked="" type="checkbox"/> 10: <input checked="" type="checkbox"/> 11: <input checked="" type="checkbox"/> 12: <input checked="" type="checkbox"/> 13: <input checked="" type="checkbox"/> 14: <input checked="" type="checkbox"/> 15: <input checked="" type="checkbox"/> 16: <input checked="" type="checkbox"/> 17: <input checked="" type="checkbox"/> 18: <input checked="" type="checkbox"/> 19: <input checked="" type="checkbox"/> <input type="button" value="save"/>		
Cab	Slot	Device Summary
<input type="button" value="view"/>	064211	CPSMM100-120 - Base Management Module Link=UP(1) Primary=YES(1) IP=172.16.46.200 Firmware="050802NA" S/N=1556124
<input type="button" value="view"/>	064213	CFETF205-205 - Fast Ethernet Twisted Pair to Fiber TP Link=DOWN(2) Fiber Link=DOWN(2)
<input type="button" value="view"/>	064214	CMEFG100-105 - 10/100/1000BaseTX to 1000BaseX 802.3ah bridge Local: Link Fiber=DOWN(2) Copper=DOWN(2) REMOTE=NOT-DETECTED(2)

Figure 37: Device Summary Screen

VIEW button:

One button for each listed card allows viewing and configuring parameters for the selected card.

Continued on next page

*Focal Point software web-based management, continued***Device details screens**

Double click the VIEW button of any card on the device summary screen to view the “Device Details” screen for that particular card. This screen shows the details of the selected card installed in the Point System chassis. See Figure 38. Configuration changes can be made to the card via this screen.

CFMFF1001314-200 - Singlemode to Multimode Fiber (Cabinet=6421 Slot=8)	
Parameter	Value (Followed by integer value from MIB, if applicable)
Group membership	<input type="text"/>
Config Match	N/A(3)
Serial Number	1611093
Enabled	Enabled(1) <input type="button" value="v"/>
Port Shutoff	DISABLED(2)
Configuration Mode	SOFTWARE(1)
Singlemode	
Signal Detect	DOWN(2)

Figure 38: Device Details Screen

Device details screen elements description

The following describes the elements of the “Device Details” screen, Figure 38.

Group Membership text field:

The “Group Membership” parameter allows adding a user-defined name in the text field. This feature is useful when changing parameters in several devices because changing the parameter in one device in a group will change the same parameter in all devices in that group.

SAVE button:

Saves the changes made to any of the parameters listed. Only those parameters that appear in text boxes or drop-down lists can be changed.

Note: Changes made at the “Device Details” screen are saved in non-volatile memory of the card(s), so the modified configuration follows the card if it is moved from one slot to another.

REFRESH button:

Click the REFRESH button to reload the current web page and to abort any unsaved changes.

Continued on next page

Focal Point software web-based management, continued

**Device details
screen elements
description
(continued)****DEVICE SUMMARY button:**

Returns to the Device Summary screen.

AGENT SUMMARY button:

Returns to the Agent Summary window.

Troubleshooting Help link:

Displays a web-based link to an integrated set of help files that provides help for using the embedded HTTP (*Web*) server software.

The help screens can be viewed and printed from any standard HTML browser.

Help-screen files are only current to the date the CD was produced. The most current files are at www.transition.com/pshelp

CPSMM100 firmware upgrades

About downloading the firmware

CAUTION: If the 'WRITE' phase is interrupted or fails for any reason while downloading the firmware, the management module will be damaged requiring factory service. Use of a battery-backed uninterruptible power supply is highly recommended.

Notes:

- The firmware download command "xr" is only available from a serial connection. The management module firmware can be upgraded via the serial port or (*by using FTP*) via a serial connection or a Telnet session.
- Firmware upgrades can cause the loss of all saved settings.
- DO NOT transfer a ZIP file. UnZIP the ZIP file and transfer the binary file contained in the ZIP file. (*Firmware files are NOT automatically extracted from ZIP files.*)

Upgrading the firmware

To upgrade the firmware, do the following:

Step	Action
1.	Obtain new firmware by contacting Transition Networks' technical support team.
2.	Start the file transfer by entering the following commands at the CLI: <ul style="list-style-type: none"> • CPSMM100> su=<password> • [su] CPSMM100> xr
3.	Press the ENTER key and the following output results: <p>DOWNLOAD: You have entered the "Upgrade Firmware" command. This process consists of two phases: 'XMODEM DOWNLOAD' and 'WRITE,' IF THE 'WRITE' PHASE IS INTERRUPTED OR FAILS FOR ANY REASON, THE MANAGEMENT MODULE WILL BE DAMAGED AND WILL NEED TO BE RETURNED TO THE FACTORY FOR SERVICE. Use of a battery-backed uninterruptible power supply is highly recommended. If you have any doubts about this process, please abort and contact technical support for assistance.</p> <p>DOWNLOAD: CAUTION: Firmware upgrade may cause all saved settings to be lost.</p> <p>DOWNLOAD: Please begin download using XMODEM/CRC protocol (128 byte blocks), or abort by pressing RESET or disconnecting power.</p>

Continued on next page

CPSMM100 firmware upgrades, continued

**Upgrading
firmware**

The firmware upgrade process is activated using three methods: “XMODEM DOWNLOAD” and “WRITE.”

Step	Action
4.	The “XMODEM DOWNLOAD” phase is activated by initiating a “Send” or “Upload” command from the terminal emulator to send the new firmware to the Management Module. In this example, a “Send” command is initiated by selecting [Transfer] [Send File] as shown in Figure 39.

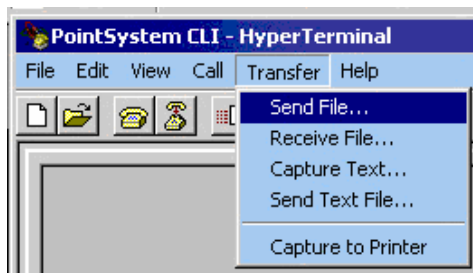


Figure 39: Point System CLI HyperTerminal

5.	When the Send File dialog box opens, select “Xmodem” from the protocol pull-down list. See Figure 40.
----	---

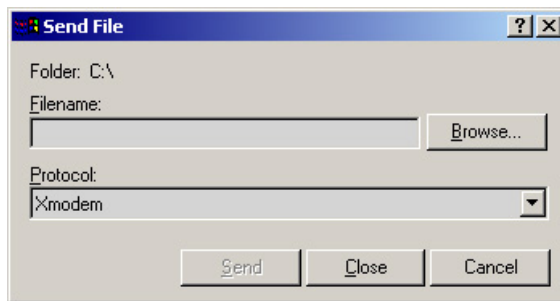


Figure 40: Send File Dialog Box

6.	Click the BROWSER button to locate the management upgrade file.
----	---

Continued on next page

CPSMM100 firmware upgrades, continued**Upgrading firmware** *(continued)*

Step	Action
7.	<p>Select the file and click the OPEN button to initiate the file transfer.</p> <ul style="list-style-type: none"> • When the “XMODEM DOWNLOAD” is complete, the write phase will start automatically. During the write phase, the agent writes the firmware upgrade to the management module. <p>CAUTION: If the write phase is interrupted or fails for any reason, the management module will be damaged, necessitating factory service. Use of a battery-backed, uninterruptible power supply is HIGHLY recommended.</p> <ul style="list-style-type: none"> • When the file transfer is complete, the new code is written into flash memory and the management module will reboot automatically.

Section III

Command-Line Interface (CLI)

Introduction

The CLI is similar to a UNIX shell prompt. It allows viewing all management data from Transition Networks' media converters and chassis.

The CLI allows troubleshooting the management Module(s)—also other stations on the network—using diagnostic commands and messages.

The CLI is accessible through the following ways:

- An attached terminal or terminal emulator connected to the DB-9 serial port.
- A remote Telnet connection via the RJ-45 Ethernet port.

Note: Both the serial driver and the Telnet driver tap into the same data stream accessed via the CLI.

In this section

These are the topics:

Topic	See Page
DB-9 serial port CLA access	40
RJ-45 Ethernet port CLA access	45
Network security	48
Configuring redundant-based management modules	57
Command-line interface references	59

DB-9 serial port CLA access

CLI access via a DB-9 serial port

CLI access via the DB-9 serial port is used in the following circumstances:

- When setting up or changing the IP configuration of the management module (*Initial IP configuration is most commonly performed at CLI via the serial port. Subsequent IP configuration changes via Telnet are supported, but strongly discouraged.*)
- When optimizing performance during a troubleshooting session.
- When upgrading firmware.

Hardware

The hardware setup begins with one or more Transition Networks' management module(s) CPSMM-200 or CPSMM-120 installed in one or more Transition Networks' Point System chassis:

- CPSMC0200-100 2-slot chassis
- CPSMC0800-100 8-slot chassis
- CPSMC13xx-100 13-slot chassis
- CPSMC18xx-xxx 18-slot chassis
- CPSMC19xx-100 19-slot chassis

Figure 41 shows a CPSMC chassis containing a management module connected to a remote terminal for management via a DB-9 serial port. See the CPSMM series manuals for specific chassis detailed information on installing the management module.

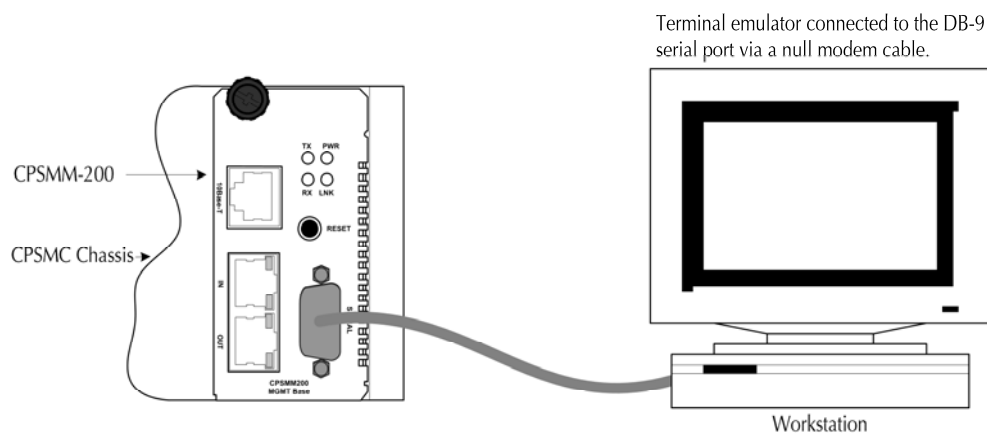


Figure 41: Terminal Emulator/MMU Connection via DB-9 Serial Port

Continued on next page

*DB-9 serial port CLA access, continued***DB-9 port
hardware setup**

To set up the hardware via the DB-9 port, do the following:

Step	Action
1.	Locate a null modem DB-9 serial port cable with a female DB-9 connector. Refer to the Cable Specifications section in this manual for the null-modem cable configuration.
2.	Attach the DB-9 serial port female cable connector to the DB-9 serial port male connector on the management module.
3.	Attach the other end of the DB-9 serial port cable to the ASCII terminal or terminal emulator.
4.	Using methods appropriate to the attached terminal, verify that the serial port parameters of the attached terminal match those of the TN chassis. If necessary, modify the port parameter values for the attached terminal emulator. The default serial port parameter values for the TN chassis are: <ul style="list-style-type: none"> • Bits per second 9600* • Stop bits 1 • Data bits 8 • Parity (<i>none</i>) * Supports 38,400 bits per second, which is changeable by using the “bps” command. See Appendix A: Command Line Interface Commands for more information.
5.	Power up the Transition Networks chassis, or press the RESET button on the management module.
6.	Press the ENTER (<i>RETURN</i>) key, depending on the terminal’s keyboard to bring up a command-line prompt on the attached terminal or terminal emulator: CPSMM100>_

Note: The default value for the console prompt string depends on the management module:

- CPSMM100-120 is the prompt for the CPSMM-120 management module.
- CPSMM100-200 is the prompt for the CPSMM-200 management module.
- CPSMM100-400 is the prompt for the management module installed in the SMACF10xx-20x media converter.

For the sake of simplicity, the console prompt was changed to “**CPSMM100>**” for all examples. The string can be changed with the MIB variable: **cpsmm100.SysName.0**

See Appendix A: “Command Line Interface Commands” for more information.

Continued on next page

DB-9 serial port CLA access, continued

IP parameters The Internet protocol (IP) network parameters are set through the DB-9 serial port via the CLI. Setting the IP parameters allows monitoring and managing the TN chassis from a remote location.

Setting IP parameters

To set IP parameters, do the following:

Step	Action
1.	For the first time, access the super-user CLI prompt using the case sensitive password “private,” and the CLI prompt will appear as shown in Figure 42.

```
stargate% tip /dev/ttya -9600
connected
CPSMM100-120> _
```

Figure 42: CLI Prompt

2.	At the CPSMM100 prompt, type <code>su=private</code> .
3.	Press the ENTER key and the super-user prompt will appear as shown in Figure 43.

```
CPSMM100-120> su=private
Super-user mode on.
[su] CPSMM100-120> _
```

Figure 43: Super-User CPSMM 100 Prompt

4.	Set the IP, netmask, and gateway addresses using this format: <code>[SU] CPSMM100> set ip=nnn.nnn.nnn.nnn</code>
5.	Set the default IP gateway (router) of the management module: <code>[SU] CPSMM100> set gateway=nnn.nnn.nnn.nnn</code>
6.	Set the local IP subnet mask to be used by the management module: <code>[SU] CPSMM100> set netmask=nnn.nnn.nnn.nnn</code>
7.	Enter the “save” command to save the network configurations: <code>[SU] CPSMM100> save</code>
8.	Enter ‘su’ to exit super-user mode: <code>[SU] CPSMM100> su</code> <code>CPSMM100> _</code>

Note: The single-command IPC can set the local IP address, subnet mask, and gateway. See Appendix A: Command Line Interface Commands for more information.

Continued on next page

DB-9 serial port CLA access, continued

Passwords The CLI provides two passwords or “community names” that have the default values: “private” and “public.”

Private password The private password is used in three specific roles:

- SNMP read/write access
- Telnet login access
- CLI super-user mode access

Public password The public password is used for read-only access in SNMP and Web in older revisions, and for read-only access in Telnet mode in more recent revisions.

Note: To change the password you must be in super user mode

Enter super-user mode To enter super-user mode, do the following:

Step	Action
1.	At the prompt type: <code>su=<your password></code>
2.	Press the ENTER/(RETURN) key and the prompt will appear similar to this: <code>[su] CPSMM100-200> _ (in Super-user mode)</code>

Exit super-user mode To exit Super-User (SU) mode, do the following:

Step	Action
1.	At the prompt type: <code>su</code>
2.	Press the ENTER/(RETURN) key and the display will show: “Super-user mode OFF”

Continued on next page

DB-9 serial port CLA access, continued**Changing passwords**

Change the Passwords by changing the default community name at the super-user prompt:

```
[su] CPSMM100> set public=<public community name>
```

```
[su] CPSMM100> set private=<community name>
```

Enter the “save” command to save the network configurations.

```
[su] CPSMM100> save
```

Note: Changing the private password or “community name” simultaneously changes both the Telnet and super-user passwords.

RJ-45 Ethernet port CLA access

CLI access via an RJ-45 Ethernet port

CLI access via the RJ-45 Ethernet port is used when CLI access is needed from a physical location other than the wiring closet where the Point System chassis is installed.

CPSMC Hardware

The hardware setup begins with one or more TN management module(s) (*CPSMM-200* or *CPSMM-120*) installed in one or more TN Point System chassis:

- CPSMC0200-100 2-slot chassis
- CPSMC0800-100 8-slot chassis
- CPSMC13xx-100 13-slot chassis
- CPSMC18xx-xxx 18-slot chassis
- CPSMC19xx-100 19-slot chassis

See Figure 44.

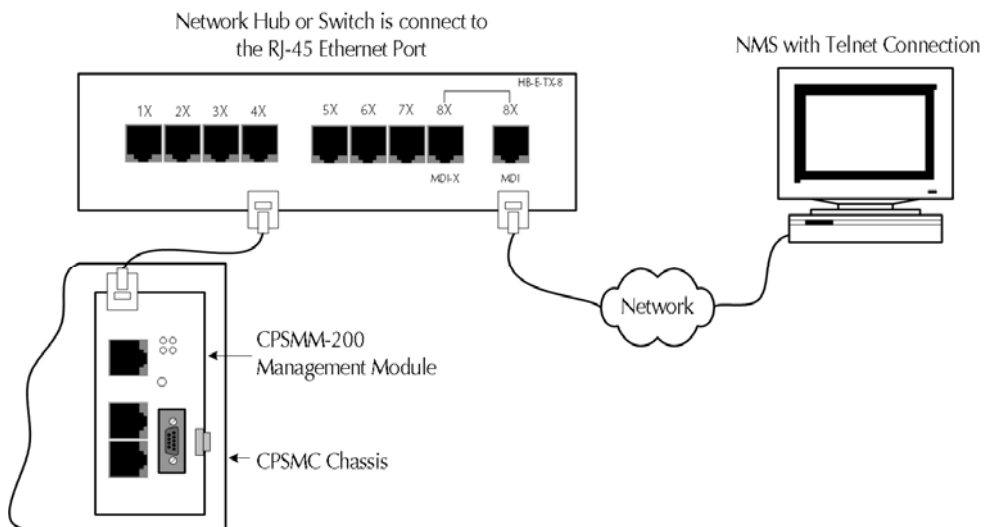


Figure 44: NMS Telnet Connection

Continued on next page

RJ-45 Ethernet port CLA access, continued**Telnet server**

The TN Point System Telnet server is embedded in the management module (*CPSMM-120 or CPSMM-200*) and allows access to the CLI from any computer that has an NMS with the following:

- Telnet client
- Access not blocked by network security

Note: The Internet protocol (IP) network parameters must first be set through the DB-9 serial port, using the CLI. (*See Setting the IP Parameters described earlier in this section for instructions on how to configure the management module for remote management.*)

Telnet server functionality

Additional functionality of the Telnet server:

- Telnet server password is the same as the private community name.
- Supports only a single connection at a time. Additional concurrent connection attempts are rejected.
- Attaches to the same console session available through the serial port. Users at the Telnet client and the serial terminal see the same messages and commands typed by other users.
- Supports firmware upgrades via Telnet and TFTP.
- IP configuration changes are possible via Telnet, but are strongly discouraged.

Note: IP configuration changes take effect immediately when commands are received. Therefore, these changes should not be made via Telnet unless you are confident that you understand the implications of an IP configuration change.

Connecting via telnet

To connect the Telnet client to the management-module server, do the following:

Step	Action
1.	At the command line type: Telnet nnn.nnn.nnn.nnn (<i>IP address</i>) brings up the password prompt, as shown in Figure 45.

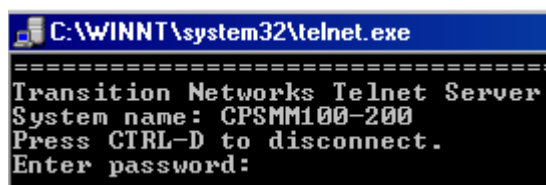


Figure 45: Password Prompt

Continued on next page

RJ-45 Ethernet port CLA access, continued**Connecting via telnet (continued)**

Step	Action
2.	At the “enter password” prompt, type the case sensitive password.
3.	Press the ENTER key to bring up the CPSMM100 prompt as shown in Figure 46.

```

Transition Networks Telnet Server
System name: CPSMM100-200
Press CTRL-D to disconnect.
Enter password:

Remote console connected to 172.16.45.88.

44:23:04:07 CPSMM100-200> _

```

Figure 46: CPSMM100-200 Prompt

Note: If you enter an incorrect password, the server immediately aborts the connection.

Terminating telnet

To disconnect the Telnet client from the management module server, press the CTRL and D keys or enter the “Logoff” command at the Telnet prompt.

Troubleshooting telnet

CLA messages specifically related to Telnet or its underlying protocols are filtered out by the Telnet server to prevent pages and pages of messages in the Telnet window. Therefore, Telnet troubleshooting should always include inspection of the command-line messages at the serial-port interface.

Network security

Preventing unauthorized access

Transition Networks has developed a set of proprietary security features that the administrator can use to prevent unauthorized access by all but the most sophisticated and determined intruders.

Network security begins when the administrator assigns unique, site-specific community name password values to replace the default private and public community name passwords.

Lock command

The lock command disables all CLI commands, but continues to allow unsolicited status messages to be displayed.

To disable all CLI commands, enter the lock command at the super-user CLI prompt as shown here: **[su] CPSMM100> lock.**

Note: After successful entry, the [locked] state is indicated at the command-line prompt: **[locked] CPSMM100>**

Though unsolicited log messages are displayed, any attempt to enter a command at any terminal results in a 'console is locked' response from the management agent.

After a lock command is issued, what happens?

Entering the "lock" command automatically saves the entire current configuration into flash memory, unless "lock" is already active in the saved configuration.

- If the CLI is locked from the serial port, a Telnet user attempting to log in would log in to a locked CLI.
 - If the CLI is locked from Telnet and later disconnected, the CLI will still be locked on reconnection.
-

How to override the lock command

To override the "lock" command and unlock the CLI, use the private community name as the default unlock password and enter the Point System "unlock" command at the super-user CLI as shown here: **[locked] CPSMM100> unlock=<password>**

Continued on next page

Network security, continued

High-security console password (HSCP)

By default the <password> is the private community name. However, since it is possible to intercept the private community name during its transmission on the network, another option is to define a High-Security Console Password (HSCP).

Defining the HSCP

To define an HSCP, enter the command:

CPSMM100> unlock=<old password>,<new HSCP>, where <old password> is the current HSCP (*if defined*), or the private community name if the HSCP is not defined.

Removing the HSCP

In order to prevent the HSCP from being intercepted, no command involving the HSCP works when a telnet session is active. Only serial port use of the HSCP is allowed. The HSCP only works with the “lock” and “unlock” commands.

To remove a previously defined HSCP, enter the following command:

CPSMM100> unlock=<HSCP>,

Note: Please note that the ending ‘comma’ of the command is required.

SNMPlock command

The “snmplock” command allows the administrator to cause the Point System agent to reject all SNMP traffic that originates outside the local subnet, unless the SNMP traffic source also has an active, logged-on Telnet session.

Since SNMP is susceptible to “IP spoofing” (*i.e., sending SNMP traffic with a bogus IP source address—a common practice among hackers*), the “snmplock” command confirms the IP source address.

After a snmplock command is issued, what happens?

When the “snmplock” command is in effect, the agent examines every incoming SNMP message.

- If the source IP for the command is on the local subnet, SNMP traffic is allowed.
 - If the source IP for the SNMP traffic is not on the local subnet, the “snmplock” command requires the agent to look for an active Telnet session.
 - If there is no active Telnet session, the SNMP traffic is denied.
 - If there is an active Telnet session, the “snmplock” command requires the agent to compare the IP address of the SNMP traffic source with the IP address of the active, logged-on Telnet session. If they match, the SNMP traffic is allowed. If they do not match, the SNMP traffic is denied.
-

Continued on next page

*Network security, continued***SNMP lock commands**

To issue a “snmplock” command at the super user prompt, do the following:

Step	Action
1.	Enter the “snmplock” command: <code>[su] CPSMM100> snmplock=YES</code>
2.	Enter the save command to save the change to flash: <code>[su] CPSMM100> save</code>
3.	At the remote location, open a Telnet session to the agent.
4.	Launch Focal Point (<i>or other SNMP application</i>) and make configuration changes to the agent.
5.	Close the Telnet session.

Terminating snmplock

To terminate the “snmplock,” which will allow SNMP traffic from any source IP whether or not Telnet is active, do the following:

Step	Action
1.	Enter the “snmplock” command: <code>[su] CPSMM100> snmplock=NO</code>
2.	Enter the “Save” command to save the change to flash memory: <code>[su] CPSMM100> save</code>

Firewall (fwall) command

The “fwall” command allows defining (*or inserting*) up to twenty rules for filtering incoming IP datagrams. Enter each rule, one at a time, via separate “fwall” commands.

Note: When the “fwall” command is active, the Point System SNMP agent does not respond to datagrams dropped due to fwall filtering (*no ICMP Destination Unreachable, TCP Reset, or any other response*).

Continued on next page

*Network security, continued***Fwall, rules for filtering incoming IP datagrams**

To insert Point System rules for filtering incoming IP datagrams, enter the “fwall” command at the “super-user” CLI prompt in the following format:

```
[su] CPSMM100> fwall=INS,<rule#>,<action>,<sip> [,<dport>[,<dprotocol>]]
```

Insert up to twenty filtering rules. Rule descriptions are listed in the table below.

Rule	Description
Rule number	An integer from one to twenty that identifies the rule.
Session	PASS to accept the datagram. DROP to discard the datagram and display a console message. SDROP to discard the datagram silently.
s(ource)IP(/mask)	Rule matching of Source IP address or subnet. "ALL" to match all IP addresses, IP address, or network number followed by network mask bit count: <ul style="list-style-type: none"> • 66.47.188.0/24 to match any IP on the 66.47.188.xxx subnet (24-bit subnet mask 255.255.255.0) • 66.47.188.206/32 to match only one IP (all 32 bits of the specified address)
d(estination) port	(Optional) If empty, the rule will match any port: value may be ALL, SNMP, Telnet, BOOTP, HTTP, or a port number in decimal. If <dport> is ICMP, then it is the ICMP type rather than a port.
d(estination) protocol	(Optional) Permitted only if <dport> is specified; if left OFF, the rule will match any protocol. The value may be ALL, ICMP, TCP, UDP, or a protocol number in decimal. See RFC1700 for values, where each rule is inserted into the slot <rule#> and all the rules that follow are moved down by one slot. The last rule is deleted, if the table is full.

Note: Rule order is significant; the first rule that matches a datagram is executed and all other rules are ignored.

IMPORTANT:

Since the “fwall=INS” command takes effect immediately, if entered incorrectly it can cause the management module to become inaccessible to the network. A message will come up urging ‘caution,’ requiring that you reenter the “fwall=INS” command within 20 seconds.

Continued on next page

*Network security, continued***Fwall, pass all traffic**

To pass all traffic, at the prompt type:

```
[su] CPSMM100> fwall=INS,I,PASS,ANY
```

Fwall, block all BOOTP

To block all BOOTP from IP 206.10.246.224 through 206.10.246.239, at the prompt type:

```
[su] CPSMM100> fwall=INS,I,SDROP,206.10.246.224/4, BOOTP
```

Fwall, show current firewall rules

fwall=SHOW:

To display current firewall rules, enter the “fwall” command at the super-user prompt in the following format:

```
[su] CPSMM100> fwall=show
```

This will bring up a site-specific display similar to:

<u>Rule#</u>	<u>Action</u>	<u>Source IP/mask</u>	<u>Protocol</u>	<u>Port/Type</u>
1	PASS	0.0.0.0/0(All)	0(All)	0(All)

Fwall, accept IP datagrams from specific hosts

fwall=LOCALSUBNETONLY:

To delete all existing firewall rules and configure the firewall to accept IP datagrams only from hosts on the local subnet, enter the “fwall” command at the super-user prompt in the following format:

```
[su] CPSMM100> fwall=LOCALSUBNETONLY
```

Fwall, accept IP datagrams from any host

fwall=WIDEOPEN:

To delete all existing firewall rules and configure the firewall to accept IP datagrams from any host, enter the “fwall” command at the super-user prompt in the following format:

```
[su] CPSMM100> fwall=WIDEOPEN
```

Fwall, eliminate gaps in rules

fwall=DEL

To delete specified rule and renumber rules to eliminate the gap, enter the “fwall” command at the super user prompt in the following format:

```
[su] CPSMM100> fwall=DEL,<rule#>
```

Note: Rule numbers range from 1 to 20.

Continued on next page

*Network security, continued***Fwall, rule positioning**

```
fwall=mov:
```

To move the rule specified by <src-rule#> so that it appears immediately before the rule currently in the position specified by <dest-rule#>, enter the “fwall” command at the super user prompt in the following format:

```
[su] CPSMM100> fwall=MOV,<src-rule#>,<dest-rule#>
```

Filtermac command

The “filtermac” command allows the administrator to specify up to four trusted Ethernet MAC addresses from which IP traffic is accepted. If no Ethernet MAC address is specified by the “filtermac” command, IP traffic will be accepted from any MAC address.

Note: The “filtermac” command does not affect non-IP traffic.

Filtermac, specify trusted Ethernet MAC address

```
filtermac=INS:
```

To specify a trusted Ethernet MAC address for accepting IP datagrams, enter the “filtermac” command at the super user prompt in the following format:

```
[su] CPSMM100> filtermac=ins,<bb.bb.bb.bb.bb.bb> (MAC address)
```

Changes take effect immediately.

Note: To determine the Ethernet address corresponding to a particular IP address, use the ping command (*which “pings” the address*), then the “arp” command (*which displays the current table of Ethernet addresses on the network*).

Filtermac, show trusted Ethernet addresses

```
filtermac=SHOW:
```

To display the current list of trusted IP datagram Ethernet addresses by the agent, enter the command: `[su] CPSMM100> filtermac=SHOW`

Press the ENTER key to bring up a site-specific display, similar to that shown below:

Rule#	Action	Source IP/Mask	Protocol	Port/Type
1	SDROP	192.251.144.3/32	0(All)	0(All)
2	SDROP	0.0.0.0/0(All)	17(UDP)	67(BOOTP)
3	SDROP	0.0.0.0/0(All)	17(UDP)	520
4	PASS	66.47.188.206/32	0(All)	0(All)
5	PASS	172.16.44.0/22	0(All)	0(All)
6	PASS	192.251.144.0/24	0(All)	0(All)
7	LDROP	0.0.0.0/0(All)	0(All)	0(All)

Continued on next page

Network security, continued

Note: If the ARP cache contains an entry for any listed Ethernet address, the IP and the MAC addresses are displayed. If the table is empty, any MAC address IP traffic is accepted.

**Filtermac,
delete Ethernet
address**

filtermac=DEL:

To delete an Ethernet address from the list of trusted Ethernet addresses, at the super user prompt type the command: **[su] CPSMM100> filtermac=DEL,<rule#>**

**Lockgw
command**

The “lockgw” command controls the way the management module handles the use of IP gateways. The “lockgw” command has three settings: “YES”, “NO” and “STRICT”.

Note: The “lockgw” command can only be set from the super user prompt.

IMPORTANT: The IP gateways send ICMP Redirect messages when they see that the management module is sending packets to the wrong gateway. When this happens, the ICMP Redirect message suggests the correct gateway. The “lockgw” command, in turn, tells the management module what to do with these suggestions.

**Set
lockgw=YES**

lockgw=YES:

To log the ICMP “Redirect” messages (*if trace is enabled*) to the default gateway address. For default and recommended settings, at the super user prompt type the following: **[su] CPSMM100> lockgw=YES**

However, datagrams destined for hosts outside the local subnet are sent to the gateway through which the most recent datagram from that address was received. This happens whether or not the ICMP Redirect message was received.

Set lockgw=NO

lockgw=NO:

To log the ICMP “Redirect” messages (*if trace is enabled*) to the gateway address as suggested by the “Redirect” message, type the following:

[su] CPSMM100> lockgw=NO

All datagrams destined for hosts outside the local subnet are sent to the default gateway. The new gateway address is not saved in non-volatile memory unless the configuration is saved through an operation such as a “save” command issued from the CLI.

Continued on next page

*Network security, continued***Set lockgw=
STRICT**

lockgw=STRICT:

To log the ICMP “Redirect” messages (*if trace is enabled*) to the gateway address as suggested by the “Redirect” message, type the following: `[su] CPSMM100> lockgw=STRICT`

This has the same function as the “lockgw=no” command “EXCEPT”: ICMP “Redirect” messages are ignored. This command may cause additional network traffic to be generated (*i.e., ICMP messages and re-forwarded datagrams*), but may slightly improve resistance to intruders using IP spoofing attacks.

**TFTPlock
command**

“TFTP” (*Trivial File Transfer Protocol*) command:

The TFTP locks or unlocks the TFTP client. Must be in super-user mode to issue a “TFTPlock” command.

TFTPlock=YES

TFTPlock=YES:

To lock the TFTP client type: `[su] CPSMM100> TFTPlock=YES`

TFTPlock=NO

TFTPlock=NO:

To unlock the TFTP client type: `[su] CPSMM100> TFTPlock=NO`

Note: This command can only be issued from the serial port. In other words, when TFTPlock is disabled, it is not possible to re-enable it via Telnet.

Continued on next page

*Network security, continued***Additional commands**

Other often used commands are as follows:

- Use the “super user” command to make high-security changes to the network parameters. (*See Setting the IP parameters.*)
su=<private password>
- Use the “set public” and “set private” commands to change the public and private passwords, respectively. Must be in super-user mode to make password changes. The format is as follows:
[su] CPSMM100> set public=<public community name>
[su] CPSMM100> set private=<community name>
- Use the “webhelp” command to change the Web location where the Point System embedded Web server looks for its help files. This command is useful in environments where Internet access is not available. The Super User mode need not be in effect.
CPSMM100> webhelp=<url>

Note: All CLI commands are listed in Appendix A: Command-Line Interface Commands.

Redundant base-management module (MMU) configuration

Redundant management modules

A Point System network can be set up with redundant management modules. When installing two base management modules into a cascaded Point System stack, the modules auto-negotiate setting one as the primary and the other as the stand-by. If the primary management module fails, the stand-by module takes over the management function automatically. See Figure 47.

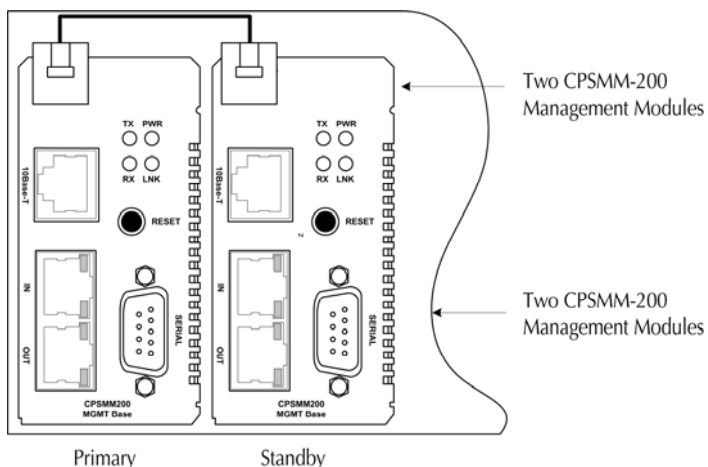


Figure 47: Redundant Management Modules

How does a base module become primary?

Base management modules become primary under the following conditions:

- If assigned a unique, valid IP configuration
- If connected to the Ethernet network

IMPORTANT:

If neither management module is set to primary, there will be no primary management module. Under this scenario, one or more cabinets may appear to the SNMP application as installed on the network, but the slide-in and power supply modules will not. Therefore, the administrator will not be able to manage those modules.

Primary module

The primary base management module scans the bus looking for other modules, queries their status, provides changes to their configurations, and accepts “SNMP,” “Web,” and “CLI” set commands.

Stand-by module

The standby base management modules listen as the primary base management module scans the bus and records maps of the stack, but cannot accept “set” commands.

Continued on next page

Redundant base-management module (MMU) configuration, continued

**Wantprimary
command**

The “wantprimary” command establishes a base management module as the primary module in a Point System chassis, giving its priority during negotiations. If multiple base management modules have their wantprimary variables set to “yes,” then these modules negotiate as equals.

**Turn
wantprimary
ON**

To turn ON the “wantprimary” command, at the prompt type:

```
CPSMM100> su=<case sensitive password>  
[su] CPSMM100> wantprimary=YES  
[su] CPSMM100> SAVE
```

**Turn
wantprimary
OFF**

To turn OFF the “wantprimary” command, at the prompt type:

```
CPSMM100> su=<case-sensitive password>  
[su] CPSMM100> wantprimary=NO  
[su] CPSMM100> SAVE
```

Note: For more information on the “primary” management module go to:
<http://www.transition.com/pshelp/redmgmt.html>

Command-line interface reference information

Introduction

The following is reference information for Transition Networks' CLI.

MIB variable breakdown

MIB variables (*also known as Managed Objects*) are referred to by a display name and the Object Identifier (OID). For example, for the variable name:

cfetf105FiberLink = 1.3.6.1.4.1.868.2.4.1.2.2.14.1.10

The display name is "cfetf100FiberLink" and the Object Identifier (OID) is the string of integers separated by decimal points.

Display name and OID

The display name and the OID are two ways of saying the same thing. The OID is the standard SNMP method of naming a variable. The display name is created as a shorthand method of representing the OID at the CLI.

Displaying MIB variables

A complete listing of the supported MIB variables is not included in this manual since the variables will change with firmware upgrades. However, you can display MIB variables by typing the "?=" command at the prompt.

Continued on next page

*Command-line interface reference information, continued***MIB variables** Example 1: Media converter MIB variables.

To display the MIB variables associated with the CFETF10xx-100 media converter, at the prompt enter this command: **CPSMM100 > ?=cfetf105**

The related MIB variables are listed below.

Display Name	Object Identifier (OID)
cfetf105Id	= 1.3.6.1.4.1.868.1.4.1.2.14
cfetf105Entry	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1
cfetf105BiaIndex	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.1
cfetf105FiberLink	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.10
cfetf105AutoNegot	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.11
cfetf105LinkPassThrough	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.12
cfetf105AutoCross	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.13
cfetf105TPActivity	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.14
cfetf105FiberActivity	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.15
cfetf105ConfigMode	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.16
cfetf105CacheClean	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.17
cfetf105SlotIndex	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.2
cfetf105Groups	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.3
cfetf105MRevision	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.4
cfetf105CfgMatch	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.5
cfetf105SerialNumber	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.6
cfetf105ConnA	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.7
cfetf105ConnB	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.8
cfetf105TPLink	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.9

Note: The MIB variables related to media converters contain a prefix of the first five letters and last three numbers of the media converter's model number.

Continued on next page

Command-line interface reference information, continued**MIB variables based on strings**

Example 2: MIB variables based on strings:

To display the MIB variables containing the string “link,” at the prompt enter this command: **CPSMM100> ?=link**

The associated MIB values are listed below.

Display Name	Object Identifier (OID)
cbftf100LinkPassThrough	= 1.3.6.1.4.1.868.2.4.1.2.2.11.1.34
cfetf100LinkPassThrough	= 1.3.6.1.4.1.868.2.4.1.2.2.14.1.12
cfetf205LinkPassThrough	= 1.3.6.1.4.1.868.2.4.1.2.2.21.1.15
cgfeb100LinkPassThrough	= 1.3.6.1.4.1.868.2.4.1.2.2.23.1.11
crmfe100LinkPassThrough	= 1.3.6.1.4.1.868.2.4.1.2.2.24.1.15
crmfe100RmtLinkPassThrough	= 1.3.6.1.4.1.868.2.4.1.2.2.24.1.30
cettf100LinkPassThrough	= 1.3.6.1.4.1.868.2.4.1.2.2.3.1.15
cfetf100LinkPassThrough	= 1.3.6.1.4.1.868.2.4.1.2.2.4.1.15
cgetf100LinkPassThrough	= 1.3.6.1.4.1.868.2.4.1.2.2.8.1.14

MIB variables of related items

Example 3: Related item MIB variables:

To display the MIB variables of all items that begin with the OID “1.3.5.1.2.1.1”, at the prompt enter this command: **CPSMM100> ?=1.3.5.1.2.1.1**

The associated MIB values are listed below.

Display Name	Object Identifier (OID)
sysDescr	= 1.3.6.1.2.1.1.1
sysObjectID	= 1.3.6.1.2.1.1.2
sysUpTime	= 1.3.6.1.2.1.1.3
sysContact	= 1.3.6.1.2.1.1.4
sysName	= 1.3.6.1.2.1.1.5
sysLocation	= 1.3.6.1.2.1.1.6
sysServices	= 1.3.6.1.2.1.1.7

Continued on next page

*Command-line interface reference information, continued***Get/set MIB values**

The operator can retrieve and/or modify the values of the MIB variables for a module using the CLI. To modify the value of the MIB variable you must know the 'serial number' of the chassis and the 'slot number' of the module.

Use the "stat" command to display the chassis serial number and module slot number. See Figure 48.

```

Transition Networks Telnet Server
System name: CPSMM100-200
Press CTRL-D to disconnect.
Enter password:

Remote console connected to 172.16.45.88.

36:03:29:52 CPSMM100-200> stat
Point System Agent Summary polltime=11.37<11.18>
CABINET: Serial=1 model=CPSMC1900-100 desc=""
  [ 1] CPSLDI00-100 - Power Indicator Card
    Supply 1=ON<1> ,INUSE<1> Supply 2=OFF<2> ,IDLE<2>
  > [ 2] CPSMM100-200 - Base Management Module
    Link=Up Primary=Y IP=192.251.144.199 F/W="060106Q7" S/N=4060828
Slot Numbers → * [ 5] CMEFG1001014-100 - 10/100/1000BaseTX to 1000BaseX 802.3ah bridge
    Local Fiber=UP<1> TP=DOWN<2> Remote=UP<1>
  * [ 8] CGETF1001013-110 - Gigabit Ethernet Twisted Pair to Fiber
    FiberLink=UP<1> TPLink=DOWN<2> Fault=YES<1>
  * [ 10] CGETF1001013-100 - Gigabit Ethernet Twisted Pair to Fiber
    FiberLink=DOWN<2> TPLink=DOWN<2> Fault=YES<1>
  * [ 11] CGETF1001013-105 - Gigabit Ethernet Twisted Pair to Fiber
    FiberLink=DOWN<2> TPLink=DOWN<2> Fault=YES<1>
  * [ 12] CRMFE1001013-200 - 100Mbps TP to Fiber w/Remote
    Local Fiber=DOWN<2> TP=DOWN<2> Remote Fiber=N/A<3> TP=N/A<3>
  * [ 13] CBFTF1001011-100 - 2 Port Ethernet Switch
    [1] Link=DOWN 100Mbps FDX ST Multimode Fiber <11>
    [2] Link=DOWN Speed/Duplex=AUTO RJ-45 <10>
  * [ 14] CGETF1001013-100 - Gigabit Ethernet Twisted Pair to Fiber
    FiberLink=DOWN<2> TPLink=DOWN<2> Fault=YES<1>
  * [ 15] CSETF1001011-200 - 10/100Mbps Twisted Pair to Fiber
    FiberLink=DOWN TPLink=DOWN Speed config=AUTO,actual=100Mbps
  * [ 16] CFETF1001013-200 - Fast Ethernet Twisted Pair to Fiber
    FiberLink=DOWN TPLink=DOWN Fault=YES AutoCross=ENABLED
  [125] CPSMP100-200 - Instant Fail Over Power Supply
    In use=YES Power_OK=YES Mode=STANDBY Load=33600mW Temp=28<C>
Prompt CPSMM100-200>

```

Figure 48: Chassis Slots Display

Note: See the breakdown of MIB variables in this section for explanations of the display name and OID.

Continued on next page

Command-line interface reference information, continued

Reading MIB variables

The operator can use either the OID number or the MIB variable name to get the MIB variable.

To read the value of a MIB variable for a module, use the “get” command. The command syntax in the two cases is as follows:

- **GET=<oid>.<Serial Number>.<Slot Number>**

or

- **GET=<MIB Variable Name>.<Serial Number>.<Slot Number>**

Figure 49 shows an example of reading the Link-Pass Through MIB for the CRMFE100 module in Slot 12:

```
CPSMM100-200> get=crmfe100linkpassthrough.1.12
SNMP: GET [192.251.144.199] id=7EB3E028 ind=0 crmfe100LinkPassThrough.1.12
Integer [1/0x1] 1/0x1
CPSMM100-200> _
```

Figure 49: Read MIB Variable CRMFE100 Module Link-Pass Through

Continued on next page

Command-line interface reference information, continued

Modifying MIB variables To modify a MIB variable for a module, login as a “super-user” and use the “set” command. The “set” command syntax is as follows:

- SET=<oid>.<Serial Number>.<Slot Number>,<type>,<value>

or

- SET=<MIB Variable Name>.<Serial Number>.<Slot Number>,<type>,<value>

Explanation of the value <type>:

<type> is the INTEGER (INT), STRING (STR), or IP

Figure 50 shows an example of a modified Link-Pass Through MIB for the CRMFE100 module on Slot 12:

```
[su] CPSMM100-200> set=crmfe100linkpassthrough.1.12,integer,1
SNMP: SET [192.251.144.199] id=7EB3E028 ind=0 crmfe100LinkPassThrough.1.12
Integer [4/0x4] 1/0x1
[su] CPSMM100-200> ▶
```

Figure 50: CRMFE100 Module Link Pass-Through MIB Variable

CLI commands See Appendix “A” for a list of CLA commands for the management module (MMU).

CLI messages See Appendix “B” for a list of CLA messages for the MMU.

Section IV:

Troubleshooting & Cable Specifications

Introduction

The following troubleshooting information is provided to assist the administrator with resolving problems with installing and using Focal Point software. If the information provided does not resolve the problem, contact technical support.

This section also provides information about cable types, cable lengths, and cable specifications.

In this section

These are the topics:

Topic	See Page
Troubleshooting problem and corrective action table	66
Cable specifications	69

Troubleshooting problem and corrective action table

Problem	Corrective Action
Focal Point software will not load	<ul style="list-style-type: none"> • The Java application may not be installed. Type the following command from the command line (<i>UNIX</i>) or the command prompt (<i>Windows</i>): C:\> java -version If the response contains the works command not found, the Java application (<i>JRE2 v1.4.0 or later</i>) must first be installed. See the Java application instructions for installation advice. • The Java application version may be too old for the current Focal Point 2.1 application. Type the following command from the command line (<i>UNIX</i>) or the command prompt (<i>Windows</i>): C:\> java -version The version displayed must be JRE v1.4.0 or later. If the version is lower, an updated Java application must first be installed. See the Java application instructions for installation advice. <p>If neither action corrects the problem, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.</p>
The Focal Point software loads, but the cabinets are not listed	<ul style="list-style-type: none"> • The connection between the NMS and the SNMP agent might not be made. Confirm that both the NMS IP address and the SNMP IP address are configured properly. Use the “ping” command to test the IP path to the SNMP agent: CPSMM100> ping=nnn.nnn.nnn.nnn If the response is: ICMP: ECHO REPLY message received from nnn.nnn.nnn.nnn Then the path is valid. (<i>The “ping” command may also be run from the NMS to the SNMP agent. The syntax is ping xxx.xxx.xxx.xxx.</i>) • If the path is valid, then the SNMP traffic may be blocked by a router or firewall. Consult your network administrator to determine if this is the case. <p>If neither action corrects the problem, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.</p>

Continued on next page

Troubleshooting problem and corrective action table, continued

Problem	Corrective Action
An unknown card error appears in the cabinet view window. However the Telnet and Web versions function normally	<ul style="list-style-type: none"> • There may be an error in the communication protocol between the hardware (I²C). To correct the problem, power-off, then power-on the chassis. • The “unknown card” may be a new type of card and, therefore, would not be included in an older revision of the SNMP agent or the Focal Point application. To correct the problem, download and install the newest revision of both SNMP and Focal Point, or contact Technical Support for assistance. <p>If neither action corrects the problem, contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.</p>
The Trap Server does not record traps	<ul style="list-style-type: none"> • Ensure the Trap Server application is running. <ul style="list-style-type: none"> ○ In the Windows environment, if the “TN” icon is displayed in the lower right corner of the monitor, then the Trap Server is running. ○ In the UNIX environments, run the “ps” command to list the processes that are currently running. If the process TN Trap Server is listed, then the Trap Server is running. • SNMP traps may be blocked by a router or a firewall. Consult your Network administrator to determine if this is the case. • The SNMP trap managers may not be configured properly. The result is the SNMP agent does not know the proper IP address. Use the “set” command to configure the trap managers. Enter the following command at the prompt: CPSMM100> set=cpsmm100SNMPTrapMgr.<cabinet serial number>.<slot number of the MM>,ip,<new IP Address of NMS> • Alternatively, use the “getnext” command to get much of this information and then use the “set=*” command to issue the set request. The following is an example. Enter “super-user mode:” CPSMM100> su=<private community name> [su] CPSMM> Enter the “getnext” command: [su] CPSMM100> getnext=cpsmm100snmptrapmgr The response is: SNMP: GETNEXT [192.251.144.229] id=D2EE6F3F ind=0 cpsmm100snmptrapmgr.1758208.1 IP Address [4/0x4] 192.251.144.235 Enter the set request: [su] CPSMM100> set=*,ip,172.16.45.105

Continued on next page

Troubleshooting problem and corrective action table, continued

Problem	Corrective Action
The Trap Server does not record traps, (<i>continued</i>)	<p>The response is:</p> <pre>SNMP: SET [192.251.144.229] id=D2EE6F3F ind=0 cpsmm100SNMPTrapMgr.1758208.1 IP Address [4/0x4] 172.16.45.105</pre> <p>Save the changes:</p> <pre>[su] CPSMM100> save</pre> <p>The response is:</p> <pre>FLASH: Saving configuration, please wait up to one minute... Writing Flash (04004500,05E8,00FE0000,00FFFFFFE) Erasing . Done Erasing/Verifying Writing [000005E8] #[0000FFFF] Done Writing Verifying FLASH: Write complete.</pre>
The Trap Viewer window exhibits strange resizing behavior	<p>This may be due to Java tool set limitations. To correct this problem, close the Trap Viewer (<i>NOT the Trap Server</i>) and re-open the Trap Viewer. This action will not affect the recording of inbound traps.</p> <p>Contact Technical Support. US/Canada: 1-800-260-1312, International: 00-1-952-941-7600.</p>

Cable specifications

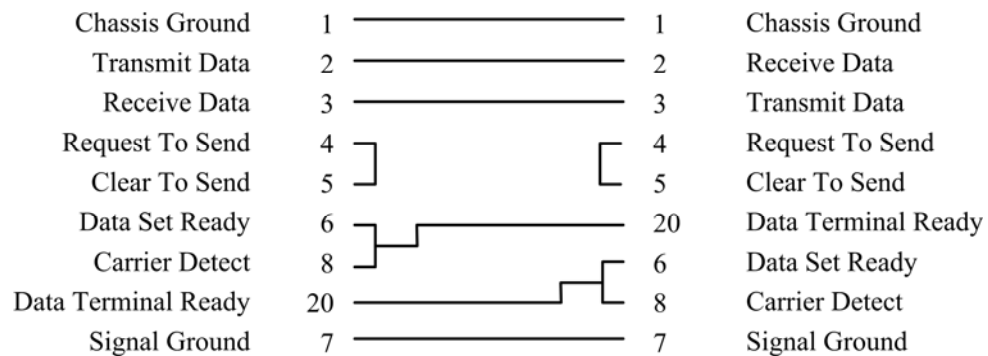
Null modem cable

Use the Null Modem cable for connecting a terminal or terminal emulator to the Management Module's DB-9 connector to access the CLI.

The table below shows the pin assignments for the DB9 cable.

Function	Mnemonic	Pin
Carrier Detect	CD	1
Receive Data	RXD	2
Transmit Data	TXD	3
Data Terminal Ready	DTR	4
Signal Ground	GND	5
Data Set Ready	DSR	6
Request To Send	RTS	7
Clear To Send	CTS	8

25 Pin RS-232 Null Modem Cable



RJ-45 cable

Category 5:

Gauge: 24 to 22 AWG
 Attenuation: 22.0 dB/100m @ 100 MHz
 Maximum Cable Distance: 100 meters

- Straight-Through or Crossover cable can be used.
- Shielded Twisted-Pair (STP) or Unshielded Twisted-Pair (UTP) can be used.
- All pin pairs (1&2, 3&6, 4&5, 7&8) are active in a Gigabit Ethernet network.
- Use only dedicated wire pairs for the active pins:
(e.g., blue/white & white/blue, orange/white & white/orange, etc.)
- DO NOT use flat or silver satin wire.

Intentionally Blank

Section V:

Contact Us & Warranty

Introduction This section explains how to contact Transition Networks: Phone, fax, email, and direct mail. It also explains what the warranty covers, who to contact to return product, and how and where to return the product.

In this section These are the topics:

Topic	See Page
Contact us	72
Warranty	73

Contact us

Technical support

Technical Support is available 24 hours a day.

United States: 1-800-260-1312

International: 00-1-952-941-7600

Live Web chat

Chat live via the Web with a Transition Networks Technical Support Specialist.

Log onto www.transition.com and click the Transition Now link.

Web-based training

Transition Networks provides 12-16 seminars per month via live web-based training.

Log onto www.transition.com and click the Learning Center link.

E-Mail

Ask a question anytime by sending an e-mail message to our technical support staff.
techsupport@transition.com

Address

Transition Networks

6475 City West Parkway

Minneapolis, MN 55344, USA

Telephone: 952-941-7600

Toll free: 800-526-9267

Fax: 952-941-2322

Warranty

Limited lifetime warranty Effective for products shipped May 1, 1999 and after. Every Transition Networks labeled product purchased after May 1, 1999 will be free from defects in material and workmanship for its lifetime. This warranty covers the original user only and is not transferable.

What the warranty does not cover This warranty does not cover damage from accident, acts of God, neglect, contamination, misuse or abnormal conditions of operation or handling, including over-voltage failures caused by use outside of the product's specified rating, or normal wear and tear of mechanical components. If the user is unsure about the proper means of installing or using the equipment, contact Transition Networks' free technical support services.

Establishing original ownership To establish original ownership and provide date of purchase, please complete and return the registration card accompanying the product or register the product on-line on our product registration page.

Transition Networks will, at its option:

- Repair the defective product to functional specifications at no charge
- Replace the product with an equivalent functional product
- Refund the purchase price of a defective product

Who to contact for returns To return a defective product for warranty coverage, contact Transition Networks' technical support department for a return authorization number. Transition's technical support department can be reached through any of the following means:

Technical Support is available 24 hours a day:

- Tel: 800-260-1312 x 200 or 952-941-7600 x 200
- Fax: 952-941-2322
- Email: techsupport@transition.com
- Live web chat: Transition Now
- Voicemail: 800-260-1312 x 579 or 952-941-7600 x 579
- All messages will be answered within one hour

Continued on next page

Warranty, continued

How and where to send the returns	<p>Send the defective product postage and insurance prepaid to the following address:</p> <p>CSI Material Management Center c/o Transition Networks 6103 Blue Circle Drive Minnetonka, MN 55343 U.S.A. Attn: RETURNS DEPT: CRA/RMA # _____</p> <p>Failure to properly protect the product during shipping may void this warranty. The return authorization number must be written on the outside of the carton to ensure its acceptance. We cannot accept delivery of any equipment that is sent to us without a CRA or RMA number.</p>
Customer pays non-compliant return costs	<p>The customer must pay for the non-compliant product(s) return transportation costs to Transition Networks for evaluation of said product(s) for repair or replacement. Transition Networks will pay for the shipping of the repaired or replaced in-warranty product(s) back to the customer (<i>any and all customs charges, tariffs, or/and taxes are the customer's responsibility</i>).</p>
Non-warranty repair costs	<p>Before making any non-warranty repair, Transition Networks requires a \$200.00 charge plus actual shipping costs to and from the customer. If the repair is greater than \$200.00, an estimate is issued to the customer for authorization of the repair. If no authorization is obtained, or the product is deemed not repairable, Transition Networks will retain the \$200.00 service charge and return the product to the customer not repaired.</p>
Repaired non-warranty products	<p>Non-warranted products that are repaired by Transition Networks for a fee will carry a 180-day limited warranty. All warranty claims are subject to the restrictions and conventions set forth by this document.</p> <p>Transition Networks reserves the right to charge for all testing and shipping incurred, if after testing, a return is classified as "No Problem Found."</p>
This warranty is your only remedy	<p>This warranty is your only remedy. No other warranties, such as fitness for a particular purpose, are expressed or implied. Transition Networks is not liable for any special, indirect, incidental or consequential damages or losses, including loss of data, arising from any cause or theory. Authorized resellers are not authorized to extend any different warranty on transition networks' behalf.</p>

Index

Cabinet View	
accessing telnet	25
agent field	24
agent/cabinet summaries	22
available cards	21
cabinet description field	23
check updates button	25
current cabinet box	24
data sheet button	23
details screen button	23, 28
device summary	22
group control string	24
help button	23
module yellow alert tags	21
power supplies one and two buttons	23
refresh button	23
tech accessing help chat	24
tech support chat button	24
telnet button	25
trap server button	26
trap viewer	26
Cable	
category 5	
Rj-45	69
specifications	
null modem	69
RJ-45	69
Card Details Dialog Box	28
Command-Line Interface	
?= command	59
access via DB-9 serial port	40
hardware setup	41
IP parameters	42
changing passwords	56
display names and OID	59
getting and setting MIB value	62
MIB variables	
based on strings	61
media converters	60
of related items	61
MIB variables breakdown	
object identifier (OID)	59
modifying MIB variables	64
reading MIB variables	63
remote access via RJ-45 ethernet port	45
DB-9 Serial Port Usage	
CLA access	40
Device Details	
data sheet button	29
group management	
group string text box	30
product manual button	29
Device Summary Screen	
description	34
Firewall Command	50
pass all traffic	52
rules and descriptions	51
WIDEPEN	52
Firmware	
CPSMM100 embedded software	4
part number	4
upgrade info	36
version content	4
Focal Point	
application setting	
security levels	15
description and features	5
features	
new for version 2.1	3
installation	11
main window pulldown menus	
file	
exit	13
help	
about	18
contents	18
tools	14
ap settings	15
collect server config	16
discover transition agents	17
nod config	16
text editor	16
trap server	15
trap viewer	15
view	
import logo image	14
refresh	14
remove logo image	14
methods of management	5
version 2.1 new features	3
web-based management	
log-in screen	31
Focal Point Mgmt.	
cabinet view	
available modules	21
cabinet view dialog box	20
set default button	20
view IP address history	19
Group Management	
group string text box	30
help button	30
Log-In Screen	

for remote management	31	models and slot counts	10
Management Module		number of slots	2
wantprimary command	58	RJ-45 Ethernet Port	
Management Modules		CLA remote access	45
primary and stand-by modules	57	telnet connection illustration.....	45
redundant module configuration.....	57	SNMP	
MIB Variables		definition.....	6
breakdown		GET/GET NEXT operations	7
display name and OID	59	management.....	6
displaying via ?= command	59	SET operation	7
get and set values.....	62	terms	6
media coverter	60	TRAP operation.....	7
modifying	64	SNMPlock Command.....	49
reading	63	Super-User Mode	
Network Security		entering and exiting	43
launch SNMPlock command	50	Telnet	
Network Security		device connecting via	46
additional commands.....	56	disconnecting	47
filtermac.....	53	server	46
filtermac command	53	to agent button	25
delete ethernet address.....	55	troubleshooting protocol.....	47
tusted ethernet addresses.....	53	Trap Server Application	26
fwall command	50	Trap Viewer	26
block all BOOTP	52	accessing help files	27
LOCALSUBNETONLY	52	Troubleshooting Focal Point	
pass all traffic.....	52	problems and corrective actions	66, 67, 68
rule positioning	53	UNIX	
fwall command rules and descriptions.....	51	Focal Point software install	11
high-security console password (HSCP)	49	Warranty	
lock command	48	how and where to send returns	74
lockgw command.....	54	non-warranty repair costs	74
override lock command	48	what's not covered	73
SNMPlock command.....	49	who to contact for returns.....	73
TFTP command	55	Web-Based Management	
New Feature		device summary screen	
get/set MIB values description	3	view button	33
getting and setting MIB values	62	log-in screen	31
Password		pointsystem agent summary screen	32
changing CLI.....	56	description field	32
network HSCP	49	group control string link	32
Point System Chassis		view button	32
hardware setup.....	10		
management system components.....	2		