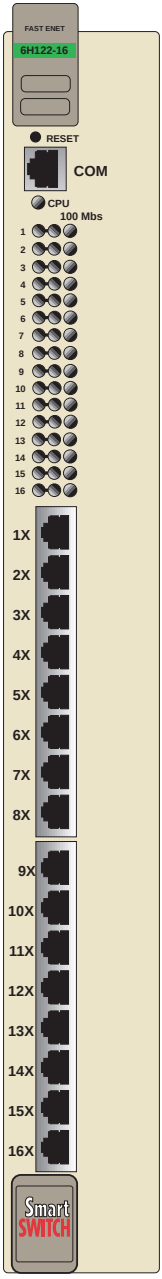
6H122-16
SmartSwitch 6000
Interface Module
User's Guide



9032361-03

CABLETRON SYSTEMS

Only qualified personnel should install the 6H122-16.

NOTICE

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Order Number: 9032361-03 October 1998

FCC NOTICE

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.

WARNING: Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

INDUSTRY CANADA NOTICE

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

VCCI NOTICE

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

CABLETRON SYSTEMS, INC. PROGRAM LICENSE AGREEMENT

IMPORTANT: Before utilizing this product, carefully read this License Agreement.

This document is an agreement between you, the end user, and Cabletron Systems, Inc. ("Cabletron") that sets forth your rights and obligations with respect to the Cabletron software program (the "Program") contained in this package. The Program may be contained in firmware, chips or other media. BY UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

CABLETRON SOFTWARE PROGRAM LICENSE

1. LICENSE. You have the right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this License Agreement.

   You may not copy, reproduce or transmit any part of the Program except as permitted by the Copyright Act of the United States or as authorized in writing by Cabletron.

2. OTHER RESTRICTIONS. You may not reverse engineer, decompile, or disassemble the Program.

3. APPLICABLE LAW. This License Agreement shall be interpreted and governed under the laws and in the state and federal courts of New Hampshire. You accept the personal jurisdiction and venue of the New Hampshire courts.

EXCLUSION OF WARRANTY AND DISCLAIMER OF LIABILITY

1. EXCLUSION OF WARRANTY. Except as may be specifically provided by Cabletron in writing, Cabletron makes no warranty, expressed or implied, concerning the Program (including its documentation and media).

   CABLETRON DISCLAIMS ALL WARRANTIES, OTHER THAN THOSE SUPPLIED TO YOU BY CABLETRON IN WRITING, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE PROGRAM, THE ACCOMPANYING WRITTEN MATERIALS, AND ANY ACCOMPANYING HARDWARE.

2. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL CABLETRON OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THIS CABLETRON PRODUCT, EVEN IF CABLETRON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, OR ON THE DURATION OR LIMITATION OF IMPLIED WARRANTIES, IN SOME INSTANCES THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU.

UNITED STATES GOVERNMENT RESTRICTED RIGHTS

The enclosed product (a) was developed solely at private expense; (b) contains “restricted computer software” submitted with restricted rights in accordance with Section 52227-19 (a) through (d) of the Commercial Computer Software - Restricted Rights Clause and its successors, and (c) in all respects is proprietary data belonging to Cabletron and/or its suppliers.

For Department of Defense units, the product is licensed with “Restricted Rights” as defined in the DoD Supplement to the Federal Acquisition Regulations, Section 52.227-7013 (c) (1) (ii) and its successors, and use, duplication, disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at 252.227-7013. Cabletron Systems, Inc., 35 Industrial Way, Rochester, New Hampshire 03867-0505.

SAFETY INFORMATION

CLASS 1 LASER TRANSCEIVERS

THE FE-100F3 FAST ETHERNET INTERFACE MODULE, FPIM-05 AND FPIM-07 FDDI PORT INTERFACE MODULES, AND APIM-29 ATM PORT INTERFACE MODULE USE CLASS 1 LASER TRANSCEIVERS. READ THE FOLLOWING SAFETY INFORMATION BEFORE INSTALLING OR OPERATING THESE MODULES.

The Class 1 laser transceivers use an optical feedback loop to maintain Class 1 operation limits. This control loop eliminates the need for maintenance checks or adjustments. The output is factory set, and does not allow any user adjustment. Class 1 laser transceivers comply with the following safety standards:

- 21 CFR 1040.10 and 1040.11 U.S. Department of Health and Human Services (FDA).
- IEC Publication 825 (International Electrotechnical Commission).
- CENELEC EN 60825 (European Committee for Electrotechnical Standardization).

When operating within their performance limitations, laser transceiver output meets the Class 1 accessible emission limit of all three standards. Class 1 levels of laser radiation are not considered hazardous.

SAFETY INFORMATION

CLASS 1 LASER TRANSCEIVERS

LASER RADIATION AND CONNECTORS

When the connector is in place, all laser radiation remains within the fiber. The maximum amount of radiant power exiting the fiber (under normal conditions) is -12.6 dBm or 55 x 10^{-6} watts.

Removing the optical connector from the transceiver allows laser radiation to emit directly from the optical port. The maximum radiance from the optical port (under worst case conditions) is 0.8 W cm^{-2} or 8 x 10^{3} W m^{2} sr-1.

Do not use optical instruments to view the laser output. The use of optical instruments to view laser output increases eye hazard. When viewing the output optical port, power must be removed from the network adapter.

DECLARATION OF CONFORMITY

Application of Council Directive(s):	**89/336/EEC** **73/23/EEC**
Manufacturer's Name:	**Cabletron Systems, Inc.**
Manufacturer's Address:	**35 Industrial Way** **PO Box 5005** **Rochester, NH 03867**
European Representative Name:	**Mr. J. Solari**
European Representative Address:	**Cabletron Systems Limited** **Nexus House, Newbury Business Park** **London Road, Newbury** **Berkshire RG13 2PZ, England**
Conformance to Directive(s)/Product Standards:	**EC Directive 89/336/EEC** **EC Directive 73/23/EEC** **EN 55022** **EN 50082-1** **EN 60950**
Equipment Type/Environment:	**Networking Equipment, for use in a Commercial or Light Industrial Environment.**

We the undersigned, hereby declare, under our sole responsibility, that the equipment packaged with this notice conforms to the above directives.

Manufacturer	Legal Representative in Europe
Mr. Ronald Fotino	Mr. J. Solari
Full Name	Full Name
Principal Compliance Engineer	Managing Director - E.M.E.A.
Title	Title
Rochester, NH, USA	Newbury, Berkshire, England
Location	Location

CONTENTS

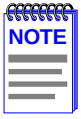
CHAPTER 5 LOCAL MANAGEMENT

CHAPTER 1
INTRODUCTION

Welcome to the Cabletron Systems **6H122-16 SmartSwitch 6000 Interface Module User's Guide**. This guide describes the 6H122-16 interface module and provides information concerning network requirements, installation, troubleshooting, and the use of Local Management.

1.1 USING THIS GUIDE

Read through this guide completely to understand the 6H122-16 module features, capabilities, and Local Management functions. A general working knowledge of Fast Ethernet and IEEE 802.3 type data communications networks and their physical layer components is helpful when using this device.



In this document, the 6H122-16 interface module is referred to as either the "6H122-16" or the "module".

1.2 STRUCTURE OF THIS GUIDE

This guide is organized as follows:

Chapter 1, **Introduction**, outlines the contents of this manual, describes the features of the 6H122-16, and provides instructions for getting additional help. This chapter also includes a list of technology and user guides that may be helpful to set up and manage the 6H122-16.

Chapter 2, **Network Requirements**, outlines the network requirements that must be met before installing the 6H122-16 into the 6C105 SmartSwitch 6000 chassis.

Chapter 3, **Installation**, provides instructions on how to install the module in the chassis and connect segments to the device.

Chapter 4, **Troubleshooting**, details the 6H122-16 LANVIEW LEDs that enable quick diagnosis of network or operational problems.

Chapter 5, **Local Management**, describes how to access Local Management and use the Local Management screens to manage the 6H122-16 module and 6C105 chassis.

Appendix A, **Specifications**, contains information on functionality and operating specifications, connector pinouts, environmental requirements, and physical properties.

Appendix B, **Mode Switch Bank Settings**, describes how to set the Mode Switches.

1.3 OVERVIEW

The 6H122-16 (Figure 1-1) is a Fast Ethernet interface module for the Cabletron Systems 6C105 chassis. The module provides sixteen RJ45 switched ports for unshielded twisted pair (UTP) cabling connectivity.

The 6H122-16 is used to connect individual high-bandwidth user devices, such as workstations, and provide a central switching point for multiple 10/100 Mbps Fast Ethernet segments.

1.3.1 Connectivity

The 6H122-16 connects to Ethernet/Fast Ethernet networks or workstations through sixteen RJ45 ports on the front panel. These ports are IEEE 802.3u 100BASE-TX compliant, and use Category 5 unshielded twisted pair cables of lengths up to 100 meters with impedances between 85 and 111 ohms.

1.3.2 Management

Management of the 6H122-16 module and 6C105 chassis and any optional equipment is accomplished using Local Management tools or remote SNMP management stations. Local Management is accessible through the front panel RS232 COM port using a local VT100 terminal, or a remote VT100 terminal via a modem connection. Local Management is also accessible in-band via a Telnet connection. In-band remote management is possible through any SNMP compliant Network Management Software.

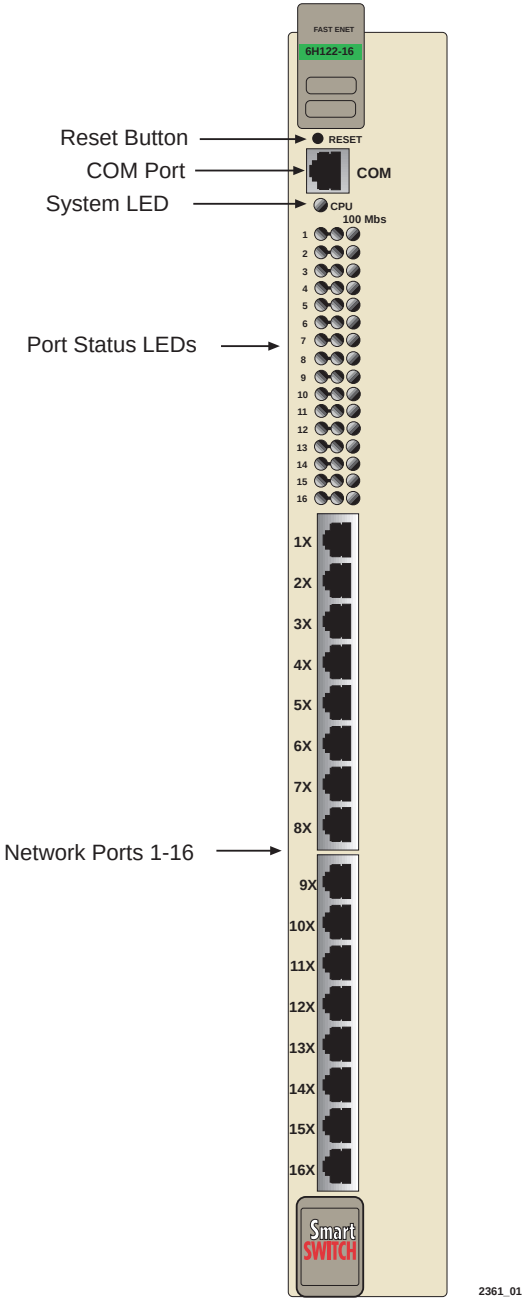


Figure 1-1 The 6H122-16

1.3.3 Distributed Chassis Management

From a management perspective, the 6C105 SmartSwitch 6000 chassis can be viewed as a single entity with a single IP address. Its management functions are distributed to all modules. This means a single module in the chassis, such as the 6H122-16, can be used to manage the entire chassis, and any other attached module through Local Management, SNMP, or Telnet applications.

1.3.4 Switching Options

The 6H122-16 provides 802.1D switching, 802.1Q switching, or SecureFast Switching Virtual Network Services between all of the front panel interfaces.

SecureFast switching and 802.1Q switching allow for future migration to Virtual Network technologies without requiring the replacement of existing equipment.

1.3.5 Full Duplex Switched Ethernet

Ports 1 through 14 support Full Duplex Switched Ethernet (FDSE) operation if the port is operating in Standard Ethernet mode (10 Mbps). This provides up to 20 Mbps of bandwidth. Ports 15 and 16 also support Full Duplex operation in Fast Ethernet mode (100 Mbps). This provides up to 200 Mbps of bandwidth.

1.3.6 Remote Monitoring

The 6H122-16 supports all Ethernet Remote Monitoring (RMON) groups, which include Statistics, Alarms, Events and History. These four groups are enabled on all ports by default.

Cabletron Systems RMON Actions is a vendor-specific extension of RMON and provides the ability to set an “Action” on any SNMP MIB variable. The Action can be triggered by any RMON Event and/or Alarm. An example of an Action would be to turn off a MIB-2 interface if a broadcast threshold is crossed.

1.3.7 SmartTrunk

SmartTrunk, also referred to as SmartTrunking, is Cabletron Systems' terminology for load balancing or load sharing. SmartTrunk technology provides an easy-to-implement mechanism to group, or aggregate, multiple physical links together to scale the backbone bandwidth beyond the limitations of a single link. All links are user-configurable so administrators can scale the backbone bandwidth by adding SmartTrunk links. The SmartTrunk benefits are as follows:

- All purchased bandwidth is used.
- Distributed, resilient links increase reliability and performance.
- Multiple technologies are supported within a single trunk for maximum flexibility.

For more information about SmartTrunk, refer to the Cabletron Systems *SmartTrunk User's Guide*.

1.3.8 Runtime IP Address Discovery

This feature enables the modules to automatically accept an IP address from a BootP server on the network into NVRAM without requiring a user to enter an IP address through Local Management.

When the modules are connected to the network and powered up, Runtime IP Address Discovery (RAD) checks the modules for an IP address. If one has not yet been assigned (module and 6C105 chassis IP address set to 0.0.0.0), RAD checks to see if any of the module interfaces have a link. If so, RAD sends out Reverse Address Resolution Protocol (RARP) and BootP requests to obtain an IP address from a RARP or BootP server on the network.

The RAD requests start out at an interval of one second. The interval then doubles after every transmission until an interval of 300 seconds is reached. At this point, the interval remains at 300 seconds. The RAD requests continue until an IP address is received from a RARP or BootP server, or an IP address is entered using Local Management.

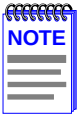
1.3.9 Port Redirect Function

The port redirect function, also referred to as “Port Mirroring,” is a troubleshooting tool used to map traffic from a single source port or multiple source ports to a destination port(s) within the chassis. This feature functions at the bit level, which allows all packets, including those with errors, to be copied and sent to an analyzer or RMON probe. The analyzer or RMON probe will see the data as if it is directly connected to the LAN segment of the source port(s).

1.3.10 Auto-Negotiation

Twisted pair ports on the 6H122-16 module have the ability to auto-negotiate the type of connection required to provide a link to another device. During Auto-Negotiation, two devices automatically exchange information “telling” each other what their operating capabilities are. The Auto-Negotiation feature targets the maximum capabilities that can be reached between the two devices. For example, the 6H122-16 adjusts to 100 Mbps when the device on the other end of the connection can also adjust between 10 Mbps or 100 Mbps. If the device on the other end of the connection can only operate at 10 Mbps, then the 6H122-16 adjusts to 10 Mbps operation.

When Auto-Negotiation is supported at both ends of a link, the two devices dynamically adjust to full or half duplex operation based on the maximum capability that can be reached between the two devices. If the device connected to the 6H122-16 cannot auto-negotiate, the 6H122-16 interface operates according to the capabilities of the other device.



All ports support standard Ethernet, standard full duplex operation, and Fast Ethernet. Ports 1 through 14 do not support Fast Ethernet in full duplex operation. However, ports 15 and 16 do support full duplex Fast Ethernet.

1.3.11 Broadcast Suppression

Broadcast Suppression allows a limit to be set on the number of receive broadcast frames per port/per second to be forwarded out the other ports on the module. Any broadcast frames above the specified limit are dropped. In the event that broadcast frames are being suppressed, multicast and unicast frames continue to be switched.

1.3.12 Standards Compatibility

The 6H122-16 is fully compliant with the IEEE 802.3u standard. The 6H122-16 provides IEEE 802.1D Spanning Tree Algorithm (STA) support to enhance the overall reliability of the network and protect against “loop” conditions. The 6H122-16 supports a wide variety of industry standard MIBs including RFC 1213 (MIB II), RFC 1757 (RMON), RFC 1493 (Bridge MIB) and RFC 1354 (FIB MIB). A full suite of Cabletron Systems Enterprise MIBs provide a wide array of statistical information to enhance troubleshooting.

1.3.13 LANVIEW Diagnostic LEDs

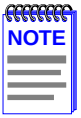
LANVIEW diagnostic LEDs serve as an important troubleshooting aid by providing an easy way to observe the status of individual ports and overall network operations. Chapter 4 provides details about the 6H122-16 LANVIEW LEDs.

1.3.14 Year 2000 Compliant

The 6H122-16 module and 6C105 chassis have an internal clock that can maintain the time and date beyond the year 1999.

1.4 DOCUMENT CONVENTIONS

The following conventions are used throughout this document:



Note symbol. Calls the reader's attention to any item of information that may be of special importance.

Tip symbol. Conveys helpful hints concerning procedures or actions.

Caution symbol. Contains information essential to avoid damage to the equipment.

Electrical Hazard Warning symbol. Warns against an action that could result in personal injury or death due to an electrical hazard.

1.5 GETTING HELP

For additional support related to this device or document, contact the Cabletron Systems Global Call Center:

World Wide Web	http://www.cabletron.com/
Phone	(603) 332-9400
Internet mail	support@cabletron.com
FTP Login Password	ftp://ftp.cabletron.com/ *anonymous* *your email address*
To send comments or suggestions concerning this document, contact the Cabletron Systems Technical Writing Department via the following email address: **TechWriting@cabletron.com** *Make sure to include the document Part Number in the email message.*	

Before calling the Cabletron Systems Global Call Center, have the following information ready:

- Your Cabletron Systems service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (e.g., changing mode switches, rebooting the unit, etc.)
- The serial and revision numbers of all involved Cabletron Systems products in the network
- A description of your network environment (layout, cable type, etc.)
- Network load and frame size at the time of trouble (if known)
- The device history (i.e., have you returned the device before, is this a recurring problem, etc.)
- Any previous Return Material Authorization (RMA) numbers

1.6 RELATED MANUALS

The following manuals may help to set up, control, and manage the 6H122-16:

Cabletron Systems *HSIM-A6DP User's Guide*

Cabletron Systems *HSIM-F6 User's Guide*

Cabletron Systems *HSIM-FE6 User's Guide*

Cabletron Systems *HSIM-W6 Installation Guide*

Cabletron Systems *HSIM-W84 Installation Guide*

Cabletron Systems *HSIM-W87 User's Guide*

Cabletron Systems *HSIM-G01/G09 User's Guide*

Cabletron Systems *Ethernet Technology Guide*

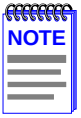
Cabletron Systems *Cabling Guide*

Cabletron Systems *Port Based VLAN User's Guide*

Cabletron Systems *SmartTrunk User's Guide*

These manuals can be obtained from the World Wide Web in Adobe Acrobat Portable Document Format (PDF) at the following site:

http://www.cabletron.com/



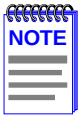
All documentation for the Cabletron Systems SecureFast VLAN Manager software is contained on the VLAN Manager CD-ROM.

The documentation for the HSIM-W6 and HSIM-W84 is on the QuickSET CD-ROM.

CHAPTER 2
NETWORK REQUIREMENTS

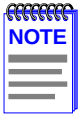
Before installing the 6H122-16, review the requirements and specifications referred to in this chapter concerning the following:

- SmartTrunk (Section 2.1)
- 10BASE-T Twisted Pair Network (Section 2.2)
- 100BASE-TX Twisted Pair Network (Section 2.3)



To ensure proper operation, use Category 5 unshielded twisted pair (UTP) cabling that has an impedance between 85 and 111 ohms.

The network installation must meet the guidelines to ensure satisfactory performance of this equipment. Failure to follow the guidelines may produce poor network performance.



The Cabletron Systems *Cabling Guide and SmartTrunk User's Guide*, can be found on the Cabletron Systems World Wide Web site: **http://www.cabletron.com/**

2.1 SmartTrunk

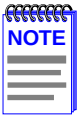
To connect the 6H122-16 to a network so it can take advantage of the SmartTrunk feature, there are certain rules concerning port connections and configurations that must be followed for proper operation. Refer to the Cabletron Systems *SmartTrunk User's Guide* for additional information.

2.2 10BASE-T NETWORK

When connecting a 10BASE-T segment to any of the 6H122-16 ports, ensure that the network meets the Ethernet network requirements of the IEEE 802.3 standard for 10BASE-T. Refer to the Cabletron Systems *Cabling Guide* for details.

2.3 100BASE-TX NETWORK

The sixteen fixed ports of the 6H122-16 provide an RJ45 connection that supports Category 5 unshielded twisted pair cabling with an impedance between 85 and 111 ohms. The device at the other end of the twisted pair segment must meet IEEE 802.3u 100BASE-TX Fast Ethernet network requirements for the devices to operate at 100 Mbps. Refer to the Cabletron Systems *Cabling Guide* for details.



The 6H122-16 is capable of operating at either 10 or 100 Mbps. The module automatically detects the speed of the other device and adjusts its speed accordingly.

CHAPTER 3
INSTALLATION

Only qualified personnel should install the 6H122-16.

This chapter covers the following items:

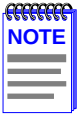
- Unpacking the 6H122-16 (Section 3.1)
- Installing the 6H122-16 into the 6C105 chassis (Section 3.2)
- Connecting to the network (Section 3.3)
- Completing the installation (Section 3.4)

3.1 UNPACKING THE 6H122-16

1. Open the box and remove the packing material protecting the module.
2. Verify the contents of the carton as listed in Table 3-1.

Table 3-1 Contents of 6H122-16 Carton

Item	Quantity
6H122-16	1
Manual Accessory Kit	1



Before proceeding with the installation, visually inspect the module for damage. If the module appears to be damaged, contact the Cabletron Systems Global Call Center. Refer to Section 1.5 for details.

3.2 INSTALLING THE 6H122-16 INTO THE 6C105 CHASSIS

Failure to observe static safety precautions could cause damage to the 6H122-16. Follow static safety handling rules and properly wear the antistatic wrist strap provided with the 6C105 chassis.

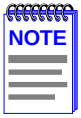
Do not cut the non-conductive bag to remove the module. Damage could result from sharp objects contacting the board or components.

The 6H122-16 can be installed in any of the 5 slots that are available. To install a module, proceed as follows:

1. Remove the blank panel covering the slot in which the module will be installed. All other slots must remain covered to ensure proper airflow and cooling. (Save the blank plate in the event you need to remove the module.)
2. Carefully remove the module from the shipping box. (Save the box and packing materials in the event the module must be reshipped.)
3. Locate the antistatic wrist strap shipped with the 6C105 chassis. Attach the strap to your wrist and plug the cable from the antistatic wrist strap into the ESD grounding receptacle at the upper right corner of the 6C105.
4. Remove the module from the plastic bag. (Save the bag in the event the module must be reshipped.) Observe all precautions to prevent damage from Electrostatic Discharge (ESD).
5. Examine the module for damage. If any damage exists, DO NOT install the module. Immediately contact the Cabletron Systems Global Call Center.

To prevent damaging the backplane connectors in the following step, take care that the module slides in straight and properly engages the backplane connectors.

6. Locate the card guides that line up with the number of the slot in which the module will be installed. Install the module in the chassis by aligning the module circuit card between the upper and lower metal card guides of the desired slot, sliding it into the chassis, and locking down the top and bottom plastic locking tabs, as shown in Figure 3-1. Take care that the module slides in straight and properly engages the backplane connectors.



When installing a module, ensure that the top plastic locking tab lines up with the desired slot number located on the front panel of the chassis. Refer to Figure 3-1.

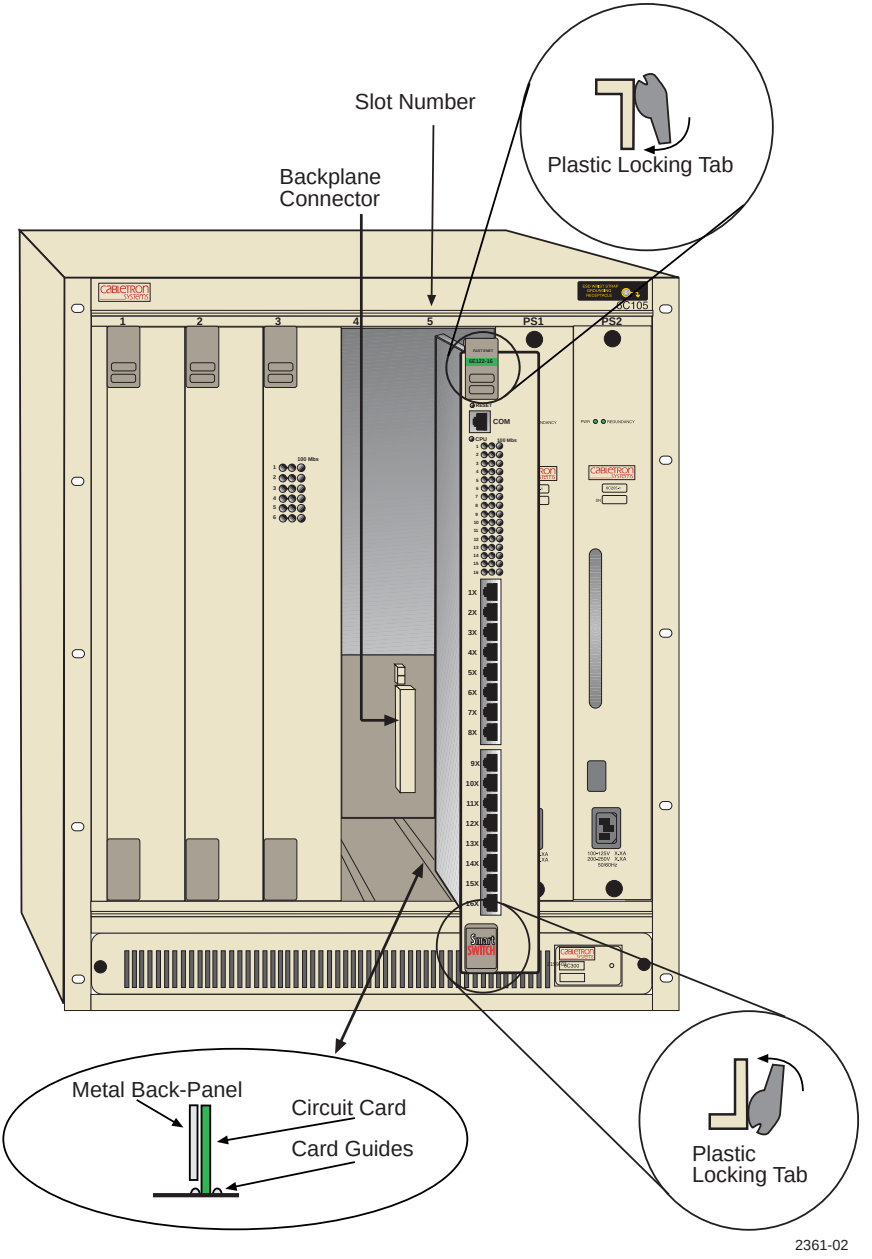
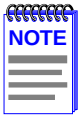


Figure 3-1 Installing an Interface Module

3.3 CONNECTING TO THE NETWORK

This section provides the procedures for connecting twisted pair segments from the network or other devices to the 6H122-16.



If the device is being installed in a network using SmartTrunking, there are rules concerning the cable connections and port connections that must be followed for SmartTrunking to operate properly. Before connecting the cables, refer to the Cabletron Systems *SmartTrunk User's Guide* for the configuration information.

Ports 1 through 16 of the 6H122-16 are 10/100 ports with internal crossovers. The ports have RJ45 connectors for twisted pair connections. When connecting a workstation, use a straight-through cable. When connecting networking devices, such as another bridge, repeater, or router, use a crossover cable. To ensure proper operation, use Category 5 unshielded twisted pair (UTP) cabling that has an impedance between 85 and 111 ohms.

To connect a twisted pair segment to the 6H122-16, proceed as follows:

1. Ensure that the device connected to the other end of the segment is powered ON.
2. Connect the twisted pair segment to the 6H122-16 by inserting the RJ45 connector on the twisted pair segment into the desired RJ45 port (Ports 1 through 16) shown in Figure 3-2.

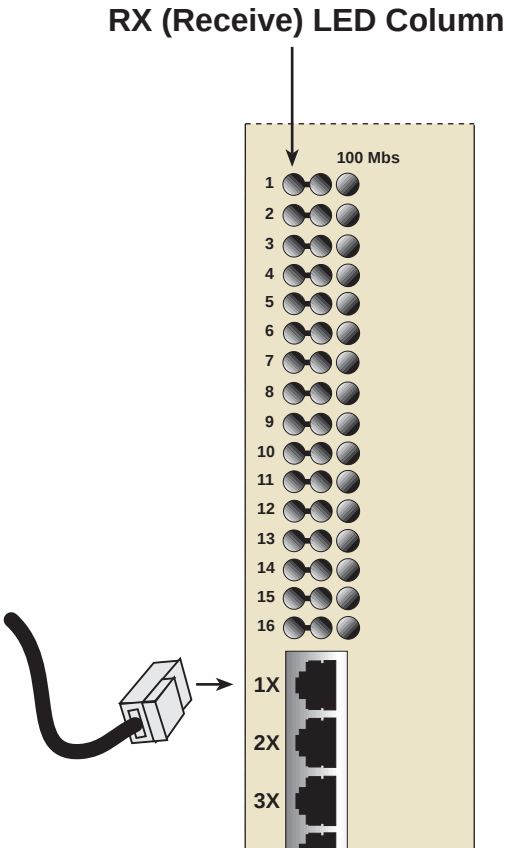


Figure 3-2 6H122-16 Twisted Pair Connection

3. Verify that a link exists by checking that the port **RX** LED is ON (flashing amber, blinking green, or solid green). If the **RX** LED is OFF and the **TX** LED is not blinking amber, perform the following steps until it is on:

   a. Verify that the device at the other end of the twisted pair segment is ON and connected to the segment.

   b. Verify that the RJ45 connectors on the twisted pair segment have the proper pinouts (Figure 3-3) and check the cable for continuity.

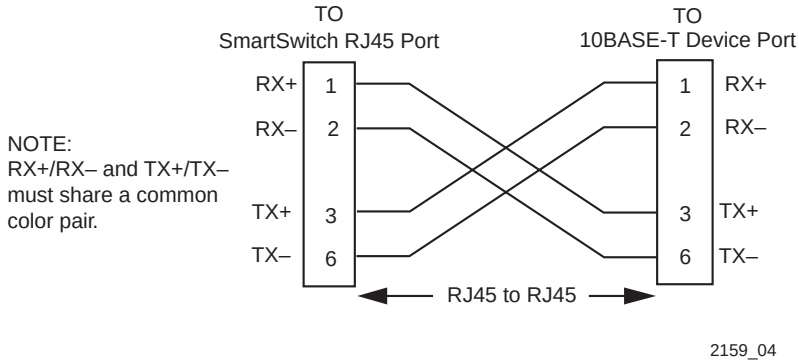


Figure 3-3 Cable Pinouts - (RJ45) Crossover Cable

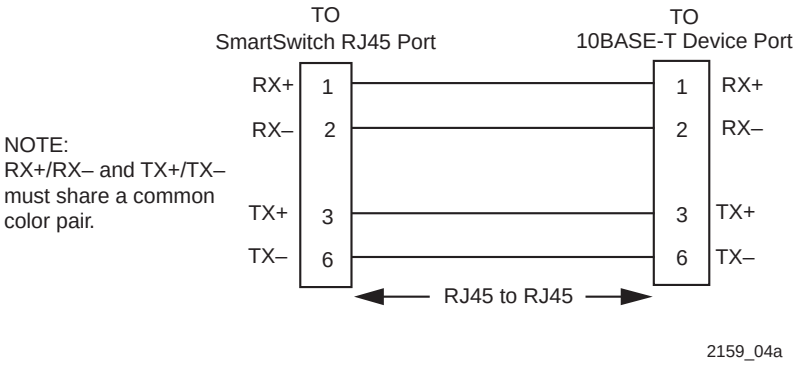


Figure 3-4 Cable Pinouts - (RJ45) Straight-Through Cable

NOTE

RX+/RX- and TX+/TX- must share a common color pair. For example, the receive pair may use the white/blue, blue/white pair, while the transmit pair may use the white/orange, orange/white pair.

c. Ensure that the twisted pair connection meets the dB loss and cable specifications outlined in the Cabletron Systems *Cabling Guide*. Refer to Section 1.5 for information on obtaining this document.

If a link is not established, contact the Cabletron Systems Global Call Center. Refer to Section 1.5 for details.

4. Repeat steps 1 through 3 above, until all connections have been made.

3.4 COMPLETING THE INSTALLATION

After installing the 6H122-16, the module is now ready to be set up through Local Management. Refer to Chapter 5 to configure the module and 6C105 chassis.

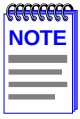
CHAPTER 4
TROUBLESHOOTING

This chapter provides information concerning the following:

- Using the LANVIEW diagnostic and status monitoring system
- Troubleshooting network and module operational problems
- Using the RESET button

4.1 USING LANVIEW

The 6H122-16 uses Cabletron Systems built-in visual diagnostic and status monitoring system called LANVIEW. The LANVIEW LEDs (Figure 4-1) allow quick observation of the network status to aid in the diagnosing of network problems. Refer to Table 4-1 for a description of the LEDs.



The terms **flashing**, **blinking**, and **solid** used in the LED definition tables of this chapter indicate the following:

Flashing indicates an irregular LED pulse.

Blinking indicates a steady LED pulse, (50% on/off).

Solid indicates a steady LED light. No pulsing.

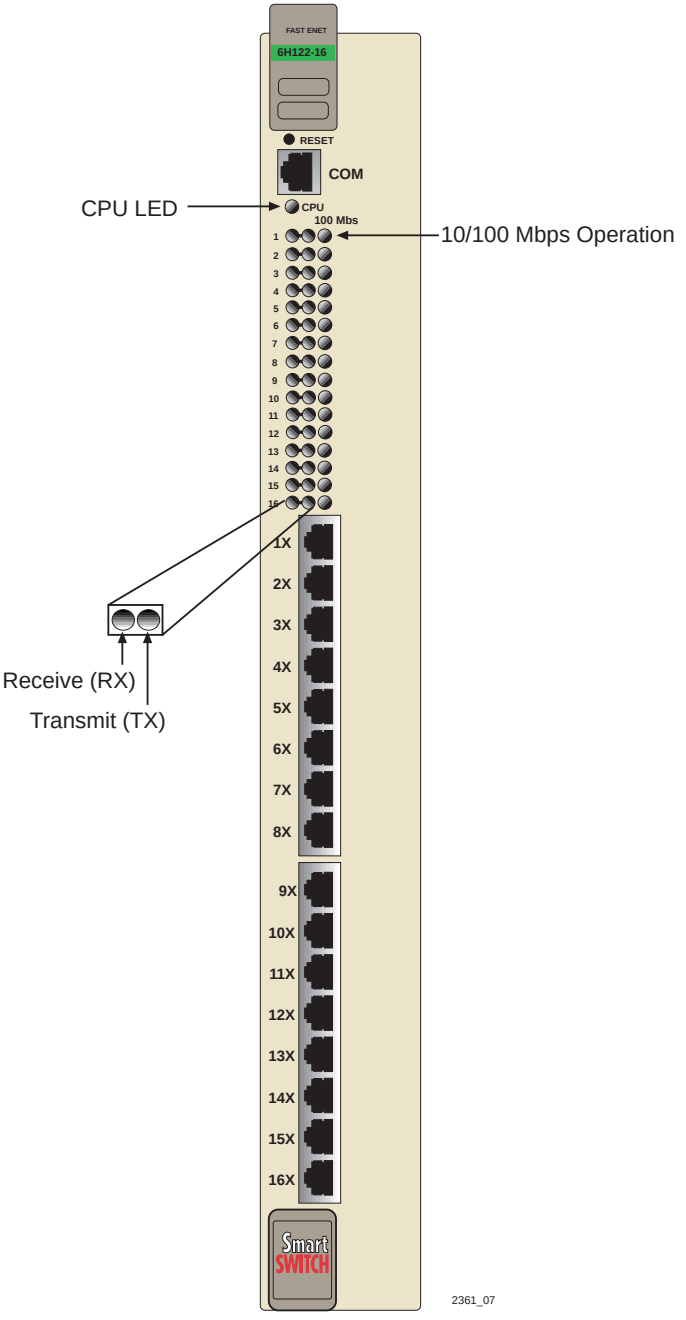


Figure 4-1 LANVIEW LEDs

Table 4-1 LANVIEW LEDs

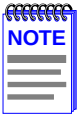
LED	Color	State	Recommended Action
CPU	Off	Power off.	Power up chassis.
	Red	**Blinking**. Hardware failure has occurred.	Contact the Cabletron Systems Global Call Center.
		Solid. Resetting, normal power up reset.	None.
	Amber	**Blinking**. Crippled.	Contact the Cabletron Systems Global Call Center.
		Solid. Testing.	None.
	Green	**Solid**. Functional.	None.
	Amber and Green	Booting. Blinks amber and green while booting.	None.
RX	Off	No link. No activity or port in Standby. Port enabled or disabled.	None.
	Green	**Solid**. Port enabled, link, no activity.	None.
		Blinking. Port disabled, link.	None.
	Amber	**Flashing**. Port enabled, link, activity.	None.
	Red	**Solid**. Diagnostic failure.	Contact the Cabletron Systems Global Call Center.

Table 4-1 LANVIEW LEDs (Continued)

LED	Color	State	Recommended Action
TX	Off	Port enabled, and no activity.	None.
	Green	**Flashing**. Indicates activity. Rate indicates data rate.	None.
	Amber	**Blinking**. Port in standby, link. Port may be disabled due to Spanning Tree.	1. Ensure that the port is not disabled (unless desired). 2. Check network design; eliminate any unnecessary loops. 3. If still not working, contact the Cabletron Systems Global Call Center.
	Red	**Flashing**. Indicates collision rate.	None, unless a high amount of activity. Check for network configuration problems or bad device.
		Solid. Diagnostic Failure.	Contact Cabletron Systems Global Call Center.

Table 4-2 Port 1-16 10/100 LED Indications

LED	Color	Description
10/100	Off	No link or no cable attached. There is a link and the port is operating at 10 Mbps operation.
	Green	Link. Port is operating at 100 Mbps.



A link exists if the associated port Receive (RX) LED is on. No link exists if the associated port Receive (RX) LED is off.

4.2 TROUBLESHOOTING CHECKLIST

If the 6H122-16 is not working properly, refer to Table 4-3 for a checklist of possible problems, causes, and recommended actions to resolve the problem.

Table 4-3 Troubleshooting Checklist

Problem	Possible Cause	Recommended Action
All LEDs are OFF.	Loss of Power to the 6C105 chassis.	Check the proper connection of the power cable and its access to a live outlet.
	The 6H122-16 not properly installed.	Check the installation. Refer to Chapter 3.
No Local Management Password screen.	Autobaud enabled, but baud rate has not been detected.	Press ENTER (RETURN) (may take up to four times).
	Terminal setup is not correct.	Refer to Chapter 5 for proper setup procedures.
	Improper console cable pinouts.	Refer to Appendix A for proper console port pinouts.
Cannot contact the 6H122-16 from in-band management.	Improper Community Names Table.	Refer to Section 5.8 for Community Names Table setup.
	The 6H122-16 does not have an IP address.	Refer to Section 5.15.1 for IP address assignment procedure.
	Port is disabled.	Enable port.
	No link to device.	Check link to device.

Table 4-3 Troubleshooting Checklist (Continued)

Problem	Possible Cause	Recommended Action
Port(s) goes into standby for no apparent reason.	The 6H122-16 detects a looped condition.	1. Review network design and delete unnecessary loops. 2. Call the Cabletron Systems Global Call Center if problem continues.
User parameters (IP address, Device and Module name, etc.) are lost when the 6H122-16 is powered down or the front panel RESET button is pressed.	Mode switch (7), NVRAM Reset, was changed sometime before either cycling power or pressing the RESET button, causing the user-entered parameters to reset to factory default settings. Clear NVRAM was set through Local Management.	1. Reenter the lost parameters as necessary. 2. Call the Cabletron Systems Global Call Center if problem continues.

4.3 USING THE RESET BUTTON

The RESET button, located near the upper plastic locking tab of the module (see Figure 4-2), resets the 6H122-16 processor without affecting the NVRAM.

CAUTION

Pressing the RESET button resets the device, and all current switching being performed by the module is halted. A module downtime of up to two minutes will result from this action.

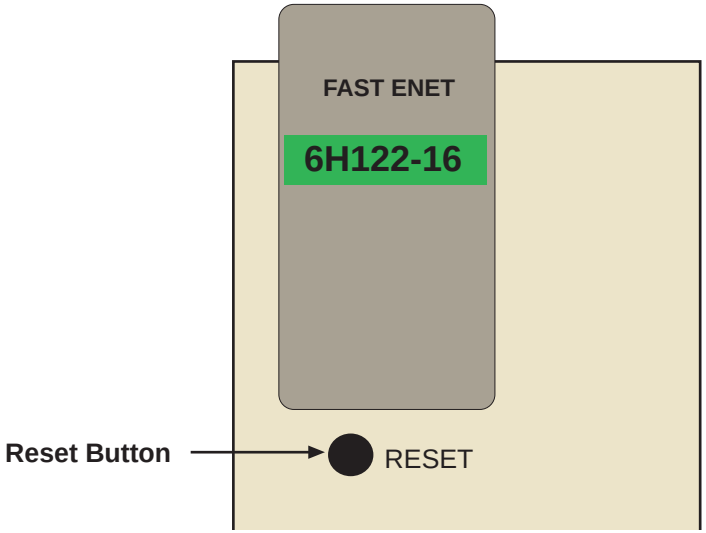


Figure 4-2 RESET Button

To reset the 6H122-16 processor, press and release the RESET button. The module processor goes through a reset process of approximately 20 seconds. Additional downtime may be added as the module reenters the network.

CHAPTER 5
LOCAL MANAGEMENT

This chapter explains how to set up a management terminal to access 6H122-16 Local Management. It also explains how to use the Local Management screens and commands.

5.1 OVERVIEW

Local Management for the 6H122-16 consists of a series of management screens that allows management of the module, the attached segments, and the 6C105 chassis. The management screens allow the following tasks to be performed:

- Manage any interface module in the chassis via a connection to a single interface module.
- Assign IP addresses and subnet masks to the 6H122-16 module, and the 6C105 chassis.
- Control access to the 6H122-16 module and the 6C105 chassis by establishing community names.
- Download a new image of operating software.
- Designate which Network Management workstations receive SNMP traps from the 6H122-16 module and the 6C105 chassis.
- Monitor the environmental status of the 6C105 chassis.
- View switch, interface, and RMON statistics.
- Assign ports to operate in standard or full duplex mode.
- Enable trunking of ports to perform load sharing.

There are three ways to access Local Management:

- Locally using a VT type terminal connected to the COM port of the 6H122-16.
- Remotely using a VT type terminal connected through a modem.
- In-band through a Telnet connection.

5.2 LOCAL MANAGEMENT KEYBOARD CONVENTIONS

All key names appear as capital letters in this manual. Table 5-1 explains the keyboard conventions and the key functions that are used.

Table 5-1 Keyboard Conventions

Key	Function
ENTER Key RETURN Key	These are selection keys that perform the same Local Management function. For example, “Press ENTER” means that you can press either ENTER or RETURN, unless this manual specifically instructs you otherwise.
ESCAPE (ESC) Key	This key allows an escape from a Local Management screen without saving changes. For example, “Press ESC twice” means the ESC key must be pressed quickly two times.
SPACE bar BACKSPACE Key	These keys cycle through selections in some Local Management fields. Use the SPACE bar to cycle forward through selections and use BACKSPACE to cycle backward through selections.
Arrow Keys	These are navigation keys. Use the UP-ARROW, DOWN-ARROW, LEFT-ARROW, and RIGHT-ARROW keys to move the screen cursor. For example, “Use the arrow keys” means to press whichever arrow key moves the cursor to the desired field on the Local Management screen.
[–] Key	This key decreases values from a Local Management increment field. For example, “Press [–]” means to press the minus sign key.
DEL Key	The DEL (Delete) key removes characters from a Local Management field. For example, “Press DEL” means to press the Delete key.

5.3 MANAGEMENT TERMINAL SETUP

Use one of the following systems to access Local Management:

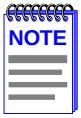
- An IBM or compatible PC running a VT series emulation software package
- A Digital Equipment Corporation VT100 type terminal
- A VT type terminal running emulation programs for the Digital Equipment Corporation VT100 series
- A remote VT100 type terminal via a modem connection
- In-band via a Telnet connection

5.3.1 Console Cable Connection

Use the Console Cable Kit provided with the 6C105 chassis to attach the management terminal to the COM port as shown in Figure 5-1.

Connect an IBM PC or compatible device, running the VT terminal emulation, to the 6H122-16 as follows:

1. Connect the RJ45 connector at one end of the cable (supplied in the kit) to the COM port on the 6H122-16.
2. Plug the RJ45 connector at the other end of the cable into the RJ45-to-DB9 adapter (supplied in the kit).
3. Connect the RJ45-to-DB9 adapter to the PC communications port.



If using a VT100 style terminal, use the RJ45 to DB25 adapter included in the Console Cable Kit, instead of the PC adapter.

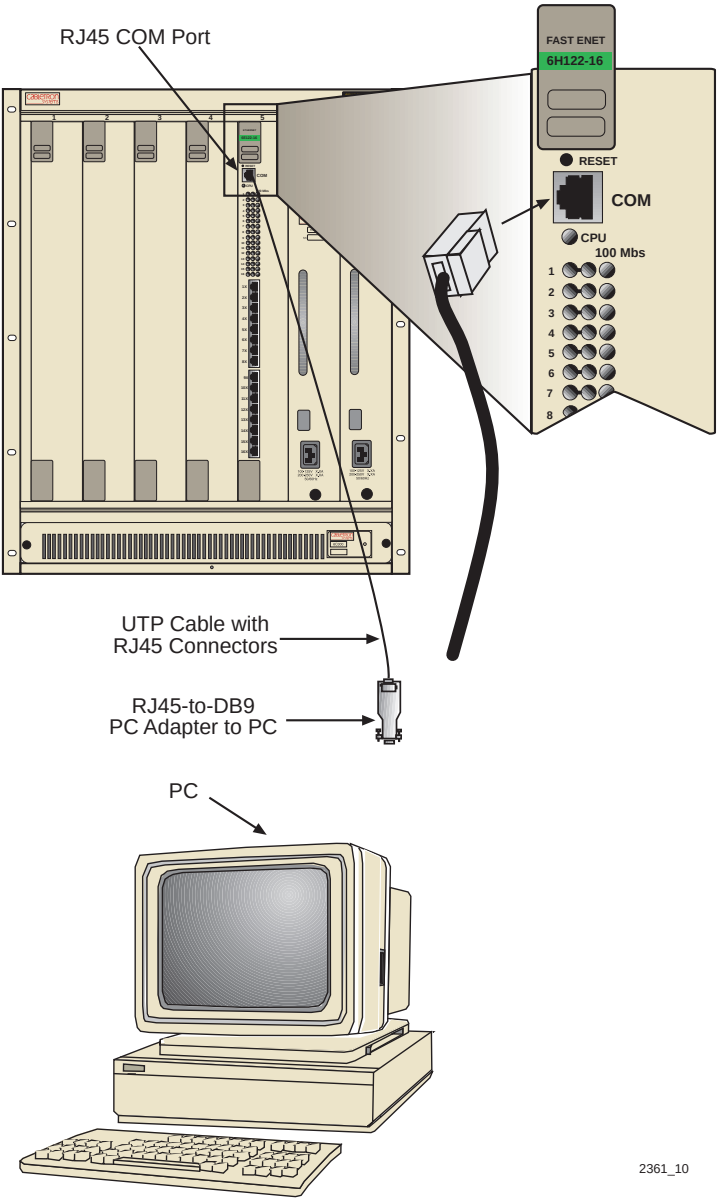


Figure 5-1 Management Terminal Connection

5.3.2 Management Terminal Setup Parameters

Table 5-2 lists the setup parameters for the local management terminal.

Table 5-2 VT Terminal Setup

Display Setup Menu	
Columns ->	80 Columns
Controls ->	Interpret Controls
Auto Wrap ->	No Auto Wrap
Scroll ->	Jump Scroll
Text Cursor ->	Cursor
Cursor Style ->	Underline Cursor Style
General Setup Menu	
Mode ->	VT100, 7 Bit Controls
ID number ->	VT100ID
Cursor Keys ->	Normal Cursor Keys
Power Supply ->	UPSS DEC Supplemental
Communications Setup Menu	
Transmit ->	2400, 4800, 9600, 19200
Receive ->	Receive=Transmit
XOFF ->	XOFF at 64
Bits ->	8 bits
Parity ->	No Parity
Stop Bit ->	1 Stop Bit
Local Echo ->	No Local Echo
Port ->	DEC-423, Data Leads Only
Transmit ->	Limited Transmit
Auto Answerback ->	No Auto Answerback
Keyboard Setup Menu	
Keys ->	Typewriter Keys
Auto Repeat ->	any option
Keyclick ->	any option
Margin Bell ->	Margin Bell
Warning Bell ->	Warning Bell

5.3.3 Telnet Connections

Once the module or chassis has a valid IP address, the user can establish a Telnet session with Local Management from any TCP/IP based node on the network. Telnet connections to the 6H122-16 require the community name passwords assigned at the SNMP Community Names screen of either the 6C105 chassis, or the module. For additional information about community names, refer to Section 5.8. Refer to the instructions included with the Telnet application for information about establishing a Telnet session.

5.3.4 Connecting an Uninterruptible Power Supply

If the 6C105 chassis is connected to an American Power Conversion (APC) Uninterruptible Power Supply (UPS) for protection from a loss of power, a connection from the COM port of a module to the UPS can be made to monitor the status of the UPS. To use the COM port for this purpose, it must be reconfigured to support the UPS application. This procedure is performed from the General Configuration screen of the interface module. Section 5.15.11, **Configuring the COM Port**, provides detailed instructions on configuring the COM port for UPS applications. Refer to the UPS documentation for details on how to access the status information.

Use the Console Cable Kit provided with the 6C105 chassis to attach the UPS to the module COM port as shown in Figure 5-2.

Connect the UPS device to the COM port of the 6H122-16 as follows:

1. Connect the RJ45 connector at one end of the cable to the COM port on the 6H122-16.
2. Plug the RJ45 connector at the other end of the cable into the RJ45-to-DB9 male (UPS) adapter, Cabletron Systems Part No. 9372066.
3. Connect the RJ45-to-DB9 male (UPS) adapter to the female DB9 port on the rear of the UPS device (refer to the particular UPS device's user instructions for more specific information about the monitoring connection).

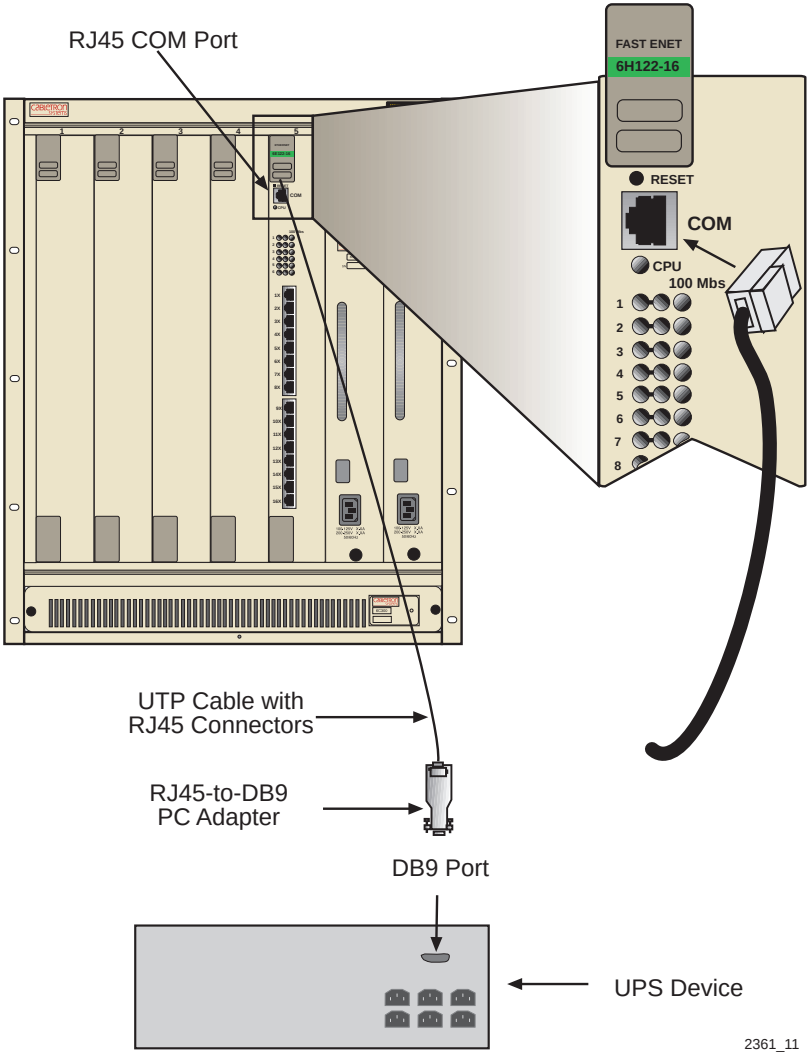


Figure 5-2 Uninterruptible Power Supply (UPS) Connection

5.4 ACCESSING LOCAL MANAGEMENT

Access to Local Management is controlled through the Password screen, Figure 5-3. Whenever a connection is made to the 6H122-16 the Password screen displays. Before continuing, the user must enter a password which is compared to the previously stored passwords. The level of access allowed the user depends on the password. To set or change passwords refer to Section 5.8. The following steps describe the procedure to access Local Management.

1. Turn on the terminal. Press ENTER (this may take up to four times, because the COM port of the 6H122-16 auto-senses the baud rate of the terminal) until the 6C105 Local Management Password screen, Figure 5-3, displays.

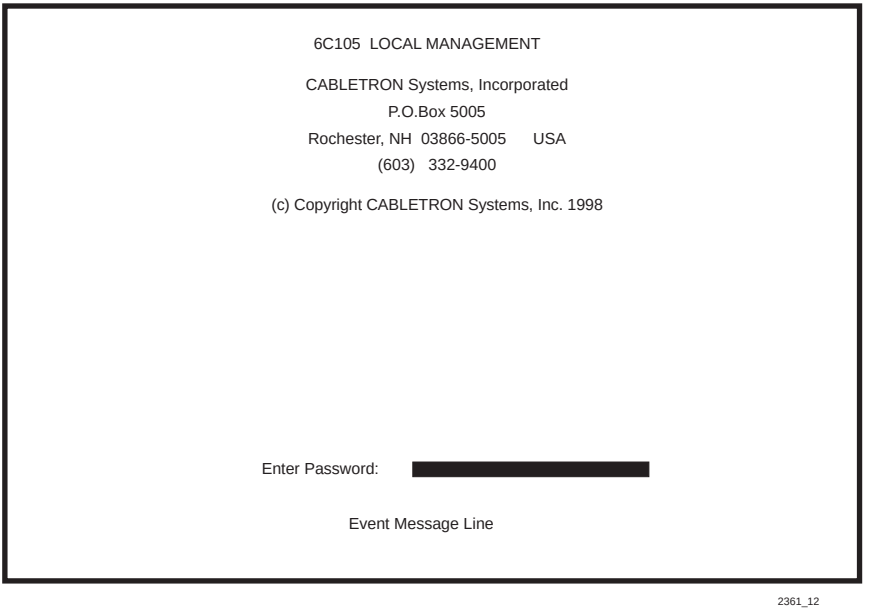
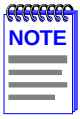


Figure 5-3 The Local Management Password Screen

2. Enter the Password and press ENTER. The default Super-User access password is "*public*" or press ENTER.



The User's password is one of the community names specified in the SNMP Community Names screen. Access to certain Local Management capabilities depends on the degree of access given to the specific community name. Refer to Section 5.8.

If an invalid password is entered, the terminal beeps and the cursor returns to the beginning of the password entry field.

Entering a valid password causes the associated access level to display at the bottom of the screen and the Main Menu screen to display.

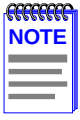
If no activity occurs for several minutes, the Password screen displays and the session ends.

5.4.1 Navigating Local Management Screens

The 6H122-16 Local Management application consists of a series of menu screens. Navigate through Local Management by selecting items from the menu screens.

The 6H122-16 supports three modes of switch operation. The switching modes are as follows:

- 802.1D SWITCHING (IEEE 802.1D switching)
- 802.1Q SWITCHING (802.1Q port based VLANs)
- SECURE FAST VLAN (Cabletron Systems SecureFast Switching)



Refer to the Release Notes shipped with the product to verify which screens are supported in each of the three available switching modes.

The switch operational mode may be set in either the Chassis Configuration screen (Section 5.7), or the General Configuration screen of the module (Section 5.15). Depending on the Operational Mode set for the module, the hierarchy of Local Management screens differs as shown in Figure 5-4, Figure 5-5, and Figure 5-6.

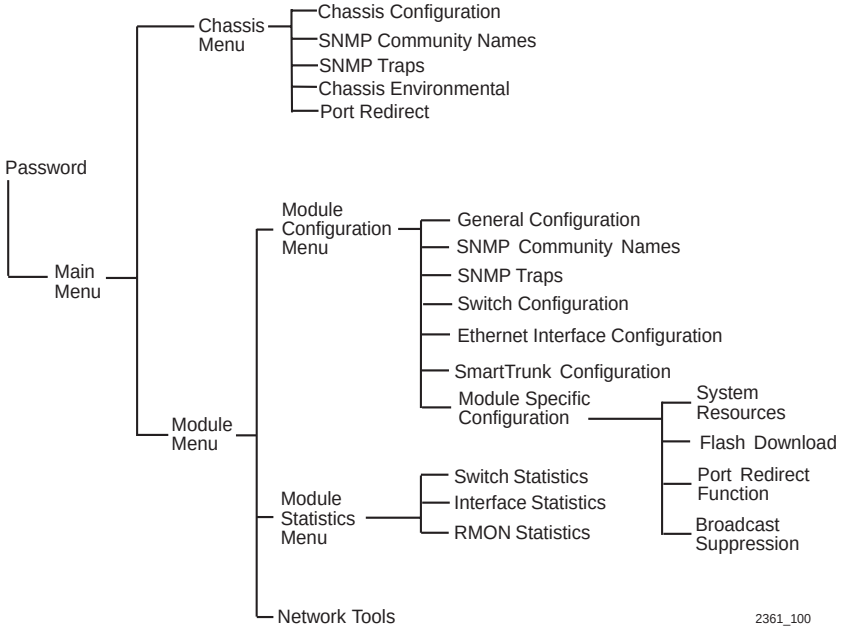


Figure 5-4 802.1D Switching Mode, LM Screen Hierarchy

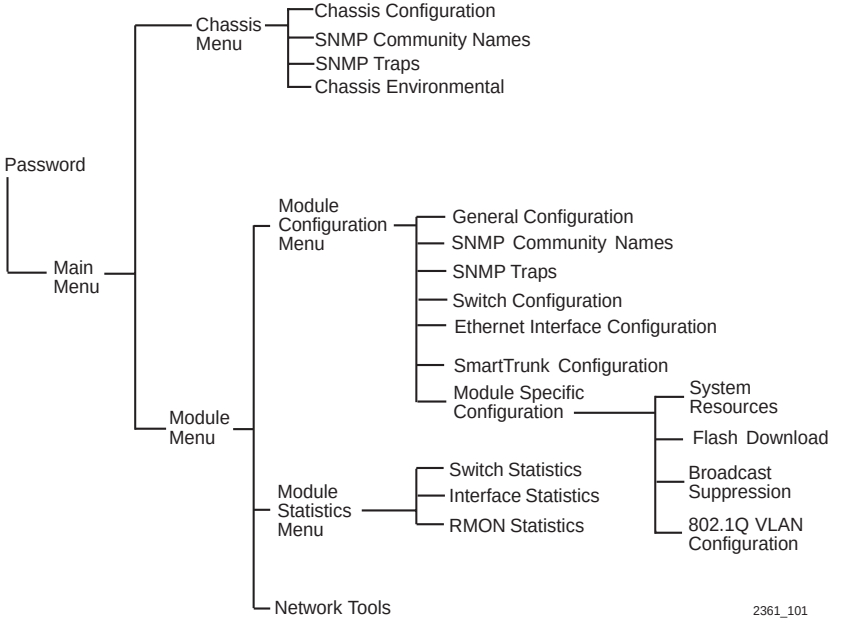


Figure 5-5 802.1Q Switching Mode, LM Screen Hierarchy

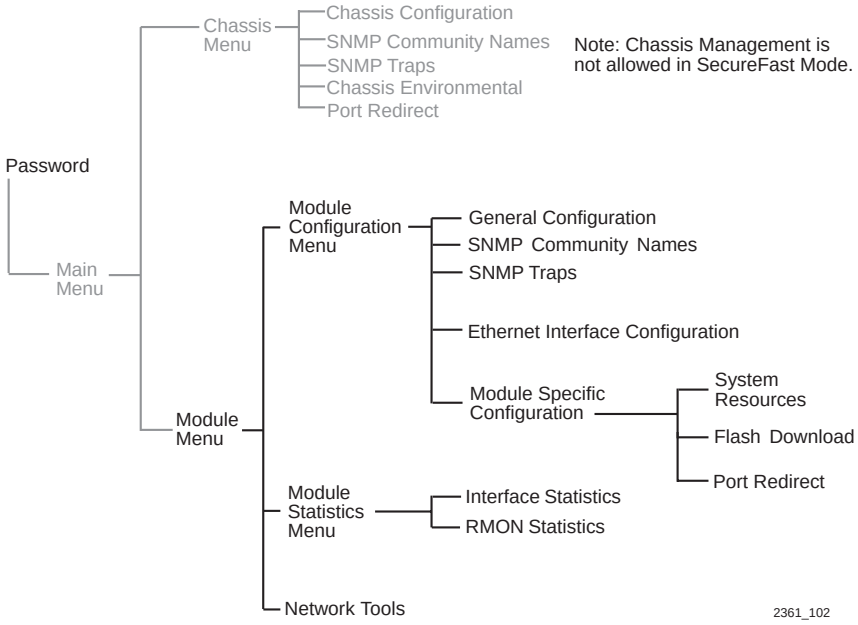


Figure 5-6 SecureFast VLAN Mode, LM Screen Hierarchy

5.4.2 Selecting Local Management Menu Screen Items

Select items on a menu screen by performing the following steps:

1. Use the arrow keys to highlight a menu item.
2. Press ENTER. The selected menu item displays on the screen.

5.4.3 Exiting Local Management Screens

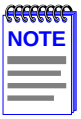
There are two ways to exit Local Management (LM), as described below.

Using the Exit Command

1. Use the arrow keys to highlight the **EXIT** command at the bottom of the Local Management screen.
2. Press ENTER. The Chassis Main Menu screen displays and the session ends.

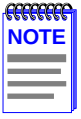
Using the Return Command

1. Use the arrow keys to highlight the **RETURN** command at the bottom of the Local Management screen.
2. Press **ENTER**. The previous screen in the Local Management hierarchy displays.



The user can also exit Local Management screens by pressing ESC twice. This exit method does not warn about unsaved changes and all unsaved changes will be lost.

3. Exit from 6H122-16 Local Management by repeating steps 1 and 2 until the chassis Main Menu screen displays.
4. Use the arrow keys to highlight the **RETURN** command at the bottom of the chassis Main Menu screen.
5. Press **ENTER**. The Password screen displays and the session ends.



If a Local Management session running on the terminal is left idle for 15 minutes, the session ends and the Local Management password screen displays. This is a normal security function, and the default lockout time can be changed by the user. See Section 5.7.6 for details.

5.5 THE MAIN MENU SCREEN

The Main Menu screen is the access point for all Local Management screens for the module and the 6C105 chassis. Figure 5-7 shows the Main Menu screen.

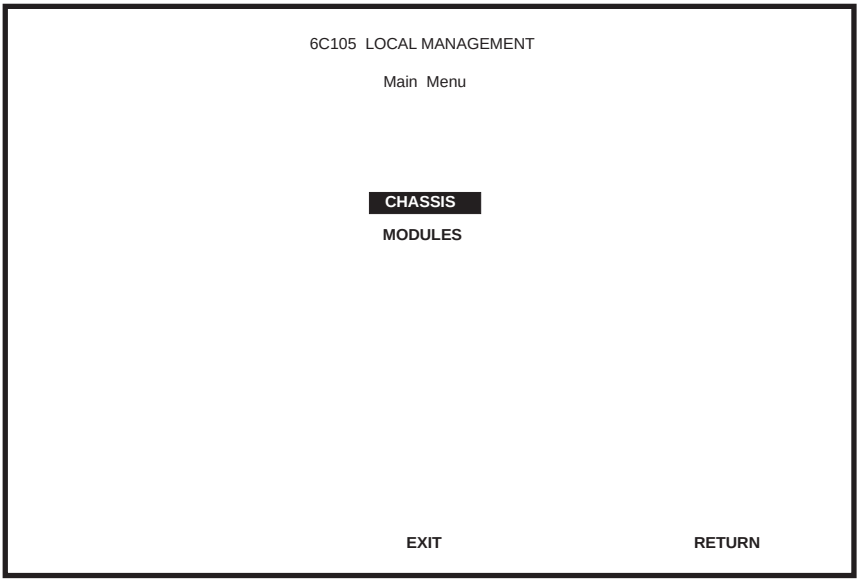


Figure 5-7 Main Menu Screen

The following explains each Main Menu screen selection as shown in Figure 5-7:

CHASSIS

The Chassis menu item provides access to the Chassis Menu screen, shown in Figure 5-8, that is used to configure the 6C105 chassis, access current chassis power supply and environmental status, and to configure IEEE 802.1Q VLANs. For details about the Chassis Menu screen, refer to Section 5.6.

MODULES

The Modules menu item provides access to the Module Selection screen that is used to select individual modules in the chassis for management purposes. For details about the Module Selection screen, refer to Section 5.12.

5.6 CHASSIS MENU SCREEN

The Chassis Menu screen, Figure 5-8, provides access to Local Management screens that allow you to configure and monitor operating parameters, modify SNMP community names, set SNMP traps, monitor the 6C105 environmental status, and perform port redirect functions.

To access the Chassis Configuration screen, use the arrow keys to highlight the **CHASSIS** menu item and press ENTER. The Chassis Configuration screen displays.

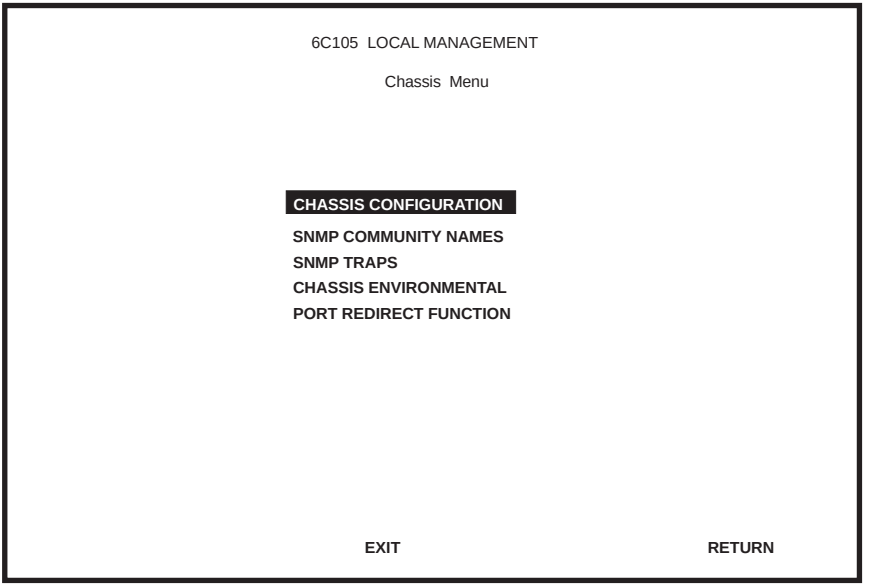


Figure 5-8 Chassis Menu Screen

The following briefly explains each screen accessible from the Chassis Menu screen.

CHASSIS CONFIGURATION

The Chassis Configuration screen enables the user to configure operating parameters for the 6C105 chassis. For details, refer to Section 5.7.

SNMP COMMUNITY NAMES

The SNMP Community Names screen allows the user to enter new, change, or review the community names used as access passwords for device management operation. Access is limited based on the password level of the user. For details, refer to Section 5.8.

SNMP TRAPS

The SNMP Traps screen provides display and configuration access to the table of IP addresses used for trap destinations and associated community names. For details, refer to Section 5.9.

CHASSIS ENVIRONMENTAL

The Chassis Environmental screen provides access to chassis power supply status, power supply redundancy status and chassis fan tray status. For details, refer to Section 5.10.

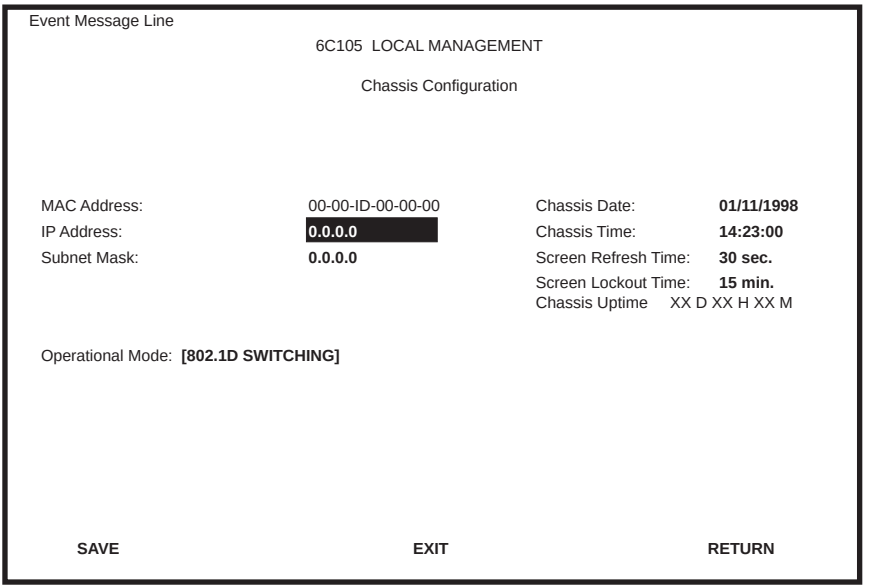
PORT REDIRECT FUNCTION

The Port Redirect Function screen allows the user to redirect traffic from one or multiple modules and ports in the chassis to a specific destination module or port. For details, refer to Section 5.11.

5.7 CHASSIS CONFIGURATION SCREEN

The Chassis Configuration screen, Figure 5-9, allows the user to set the chassis date and time, IP address and Subnet Mask, the operational mode of all modules installed in the chassis, and to view the chassis uptime.

To access the Chassis Configuration screen from the Chassis Menu screen, use the arrow keys to highlight the **CHASSIS CONFIGURATION** menu item and press ENTER. The Chassis Configuration screen, Figure 5-9, displays.



2361_41

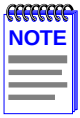
Figure 5-9 Chassis Configuration Screen

The following briefly explains each Chassis Configuration screen field:

MAC Address (Read-Only)
Displays the base physical address of the chassis.

IP Address (Modifiable)
This field allows the IP address to be set for the 6C105 chassis. If an IP address is assigned to the 6C105 chassis all the interface modules installed in the chassis can be managed via this IP address, eliminating the need to assign an IP address to each interface module. To set the IP address, refer to Section 5.7.1.

Subnet Mask (Modifiable)



When a valid IP address is assigned, the Subnet Mask field automatically enters the default mask that corresponds with class of IP entered in the IP Address field. Some firmware revisions do support changing the chassis subnet mask from the default value. Refer to your Release Notes to ensure that the Subnet Mask is a modifiable field.

Displays the subnet mask for the chassis. A subnet mask "masks out" the network bits of the IP address by setting the bits in the mask to 1 when the network treats the corresponding bits in the IP address as part of the network or subnetwork address, or to 0 if the corresponding bit identifies the host. The 6C105 chassis automatically uses the default subnet mask that corresponds to the IP class that was entered in the IP address field. Section 5.7.2 describes how to change the subnet mask from the default value.

Chassis Date (Modifiable)
Contains a value that the chassis recognizes as the current date. When the chassis date is modified, all interface modules installed in the chassis are set to this date. To set a new chassis date, refer to Section 5.7.3.

Chassis Time (Modifiable)
Contains a value that the chassis recognizes as the current time. When the chassis time is modified and saved, all interface modules installed in the chassis are set to this time. To enter a new time, refer to Section 5.7.4.

Screen Refresh Time (Modifiable)
Contains the rate at which the screens are updated. This setting determines how frequently (in seconds) information is updated on the screen. To enter a new update time, refer to Section 5.7.5.

Screen Lockout Time (Modifiable)
Contains the maximum number of minutes that the Local Management application displays a module's screen while awaiting input or action from a user. For example, if the number 5 is entered in this field, the user has up to five minutes to respond to each of the specified module's Local Management screens. In this example, after five minutes of "idleness" (no input or action), the terminal "beeps" five times, the Local Management application terminates the session, and the display returns to the Password screen. To enter a new lockout time, refer to Section 5.7.6.

Chassis Uptime (Read-Only)
Displays the total time the chassis has been operating. The chassis uptime is based on which interface module installed in the chassis has been operating for the longest period of time.

Operational Mode (Toggle)
This field allows the user to set all the modules in the chassis to operate as traditional switches (802.1D SWITCHING option), or as IEEE 802.1Q switches (802.1Q SWITCHING option).

In 802.1D SWITCHING mode, the 16 ports located on the front panel are bridged to each other.

When the operational mode is set to 802.1Q SWITCHING, the 6H122-16 acts as an IEEE 802.1Q switch. The module can be configured to increase its switching functionality by creating and maintaining port based Virtual LANs (VLANs).

For details on how to select the Operational Mode, refer to Section 5.7.7.

5.7.1 Setting the IP Address

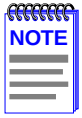
To set the IP address, perform the following steps:

1. Use the arrow keys to highlight the **IP Address** field.
2. Enter the IP address into this field using Decimal Dotted Notation (DDN) format.

   For example: 134.141.79.120
3. Press ENTER. If the IP address is a valid format, the cursor returns to the beginning of the IP address field. If the entry is not valid, the Event Message Line displays “INVALID IP ADDRESS OR FORMAT ENTERED”. Local Management does not alter the current value and refreshes the IP address field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The “SAVED OK” message displays indicating that the changes have been saved to memory.

5.7.2 Setting the Subnet Mask

If the management workstation that is to receive SNMP traps from the 6C105 is located on a separate subnet, the subnet mask for the 6C105 must be changed from its default.



When a valid IP address is assigned, the Subnet Mask field automatically enters the default mask that corresponds with class of IP entered in the IP Address field. Some firmware revisions do support changing the chassis subnet mask from the default value. Refer to your Release Notes to ensure that the Subnet Mask is a modifiable field.

To change the subnet mask from its default, perform the following steps:

1. Use the arrow keys to highlight the **Subnet Mask** field.
2. Enter the subnet mask into this field using Decimal Dotted Notation (DDN) format.

   For example: 255.255.255.0
3. Press ENTER. If the subnet mask is valid, the cursor returns to the beginning of the Subnet Mask field. If the entry is not valid, the Event Message Line displays “INVALID SUBNET MASK OR FORMAT ENTERED”. Local Management does not alter the current value, but it does refresh the Subnet Mask field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The changes are saved to memory.

5.7.3 Setting the Chassis Date

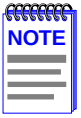
The 6C105 is year 2000 compliant, so the Chassis Date may be set beyond the year 1999. To set the chassis date, perform the following steps:

1. Use the arrow keys to highlight the **Chassis Date** field.
2. Enter the date in this format: MM/DD/YYYY

It is not necessary to add separators between month, day, and year numbers. For example, to set the date to 01/17/1998, type “01171998” in the Chassis Date field.

3. Press ENTER to set the system calendar to the date in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the date entered is a valid format, the Event Message Line at the top of the screen displays “SAVED OK”. If the entry is not valid, Local Management does not alter the current value, but it does refresh the Chassis Date field with the previous value.

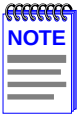


Upon saving the new chassis date, all interface modules installed in the chassis recognize the new value as the current date.

5.7.4 Setting the Chassis Time

To set the chassis clock, perform the following steps:

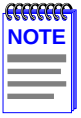
1. Use the arrow keys to highlight the **Chassis Time** field.
2. Enter the time in a 24-hour format: HH:MM:SS



When entering the time in the Chassis Time field, separators between hours, minutes, and seconds do not need to be added as long as each entry uses two numeric characters. For example, to set the time to 6:45 A.M., type “064500” in the Chassis Time field.

3. Press ENTER to set the system clock to the time in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is a valid format, the Event Message Line at the top of the screen displays “SAVED OK”. If the entry is not valid, Local Management does not alter the current value and refreshes the Chassis Time field with the previous value.



Upon saving the new chassis time, all interface modules installed in the chassis recognize the new value as the current time.

5.7.5 Entering a New Screen Refresh Time

The screen refresh time is set from 3 to 99 seconds with a default of 3 seconds. To set a new screen refresh time, perform the following steps:

1. Use the arrow keys to highlight the **Screen Refresh Time** field.
2. Enter a number from 3 to 99.
3. Press ENTER to set the refresh time to the time entered in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is within the 3 to 99 seconds range, the Event Message Line at the top of the screen displays “SAVED OK”. If the entry is not valid, the Event Message Line displays “PERMISSIBLE RANGE: 3...99” momentarily. Local Management does not alter the current setting, but it does refresh the Screen Refresh Time field with the previous value.

5.7.6 Setting the Screen Lockout Time

The screen lockout time can be set from 1 to 30 minutes with a default of 15 minutes. To set a new lockout time, perform the following steps:

1. Use the arrow keys to highlight the **Screen Lockout Time** field.
2. Enter a number from 1 to 30.
3. Press ENTER to set the lockout time in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is within the 1 to 30 minutes range, the Event Message Line at the top of the screen displays “SAVED OK”. If the entry is not valid, the Event Message Line displays “PERMISSIBLE RANGE: 1...30” momentarily. Local Management does not alter the current setting, but it does refresh the Screen Lockout Time field with the previous value.

5.7.7 Setting the Operational Mode

To set the Operational Mode, proceed as follows:

1. Use arrow keys to highlight the **Operational Mode** field.
2. Press the SPACE bar to step to the appropriate operation mode (**802.1D SWITCHING** or **802.1Q SWITCHING**).
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER. The following warning screen displays:

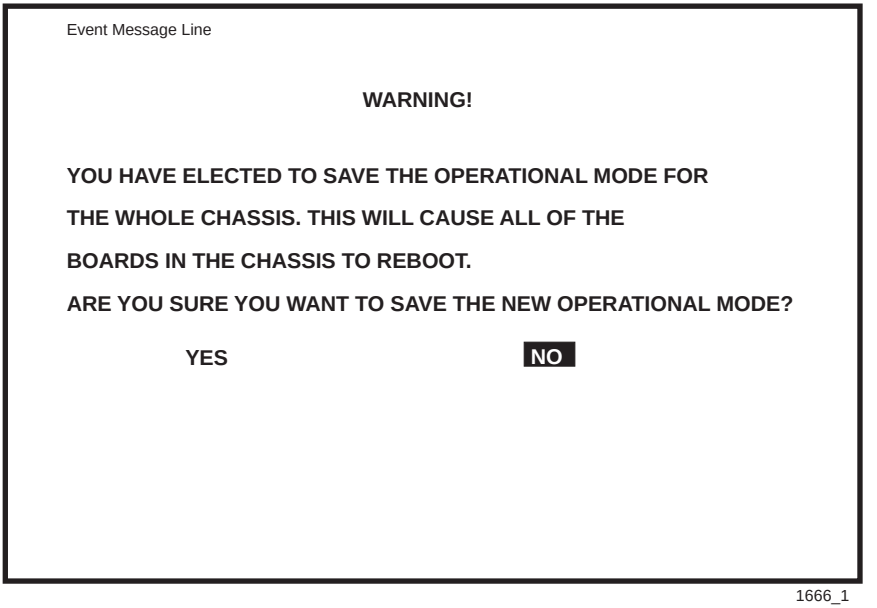
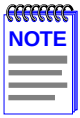


Figure 5-10 Operational Mode Warning Screen

4. Use the arrow keys to highlight the **YES** command and press ENTER. The changes are saved, and all the modules installed in the chassis reboot.

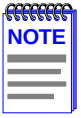


If the 6H122-16 has been set to **802.1Q SWITCHING**, refer to your *Port Based VLAN User's Guide* to configure the devices for this type of operation.

The Operational Mode field in the Chassis Configuration screen does not support the **SECURE FAST VLAN** operational mode. For the modules to function as SecureFast switches, they must have unique IP addresses, and be configured to act as Standalone devices in terms of Local Management via the 6C105 chassis. Section 5.15.9 provides additional instructions and rules that must be met before configuring the modules as SecureFast switches.

5.8 SNMP COMMUNITY NAMES SCREEN

The SNMP Community Names menu item allows the user to set Local Management community names. Community names act as passwords to Local/Remote Management and provide security access to the 6C105. Access to the 6C105 is controlled by enacting any of three different levels of security authorization (read-only, read-write, and super-user).



Super-User access gives the user full management privileges, allows existing passwords to be changed, and all modifiable MIB objects for the Cabletron Container MIB and Internet MIB-II to be edited.

To access the SNMP Community Names screen from the Chassis Menu screen, use the arrow keys to highlight the **SNMP COMMUNITY NAMES** menu item and press ENTER. The SNMP Community Names screen, Figure 5-11, displays.

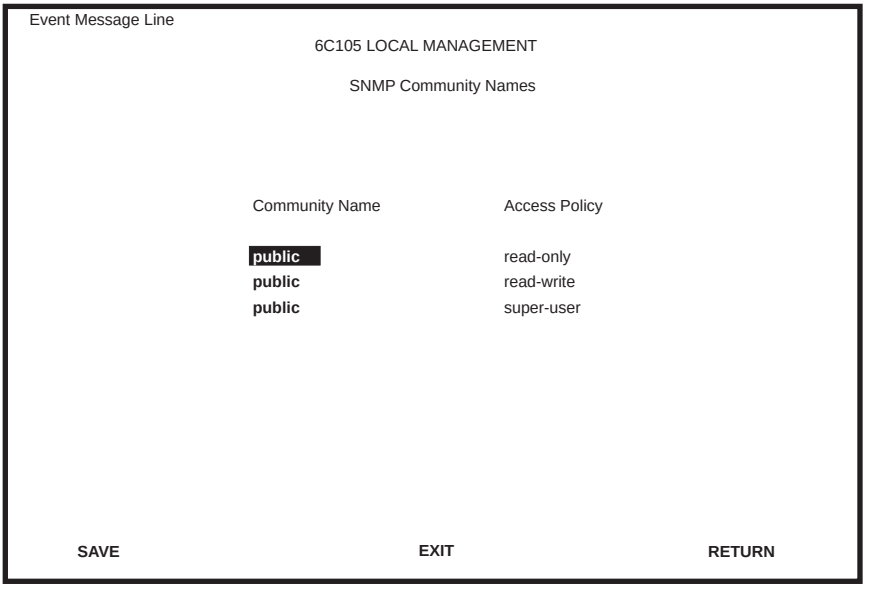


Figure 5-11 SNMP Community Names Screen

The following explains each SNMP Community Names screen field:

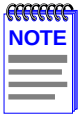
Community Name (Modifiable)
Displays the user-defined name through which a user accesses 6C105 management. Any community name assigned here acts as a password to Local/Remote Management.

Access Policy (Read-Only)
Indicates the access accorded each community name. Possible selections are as follows:

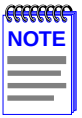
read-only	This community name allows read-only access to the 6C105 MIB objects, and excludes access to security-protected fields of read-write or super-user authorization.
read-write	This community name allows read and write access to the 6C105 MIB objects, excluding security protected fields for super-user access only.
super-user	This community name permits read-write access to the 6C105 MIB objects and allows the user to change all modifiable parameters including community names, IP addresses, traps, and SNMP objects.

5.8.1 Establishing Community Names

The password used to access Local Management at the Password screen must have Super-User access in order to view and edit the SNMP Community Names screen. Using a password with read-only or read-write access does not allow the user to view or edit the SNMP Community Names screen.



Any community name assigned in the SNMP Community Names screen is a password to its corresponding level of access to Local Management. The community name assigned Super-User access is the only one that gives the user complete access to Local Management.



All passwords assigned in the 6C105 SNMP Community Names screen allow access to both the 6C105 Local Management screens, and the Local Management screens of the interface modules that are installed in the chassis. To configure the interface module to disallow access to the 6C105 Local Management screens, refer to Section 5.16.

To establish community names, proceed as follows:

1. Use the arrow keys to highlight the **Community Name** field adjacent to the selected access level.
2. Enter the password in the field (maximum 31 characters).
3. Press ENTER.
4. Repeat steps 1 through 3 to modify the other community names.
5. Use the arrow keys to highlight **SAVE** at the bottom of the screen and press ENTER. The message “SAVED OK” displays. The community names are saved to memory and their access modes implemented.

5.9 SNMP TRAPS SCREEN

Since the 6C105 is an SNMP compliant device, it can send messages to multiple Network Management Stations to alert users of status changes. The SNMP Traps screen is shown in Figure 5-12.

To access the SNMP Traps screen from the Chassis Menu screen, use the arrow keys to highlight the **SNMP TRAPS** menu item and press ENTER. The Chassis SNMP Traps screen displays.

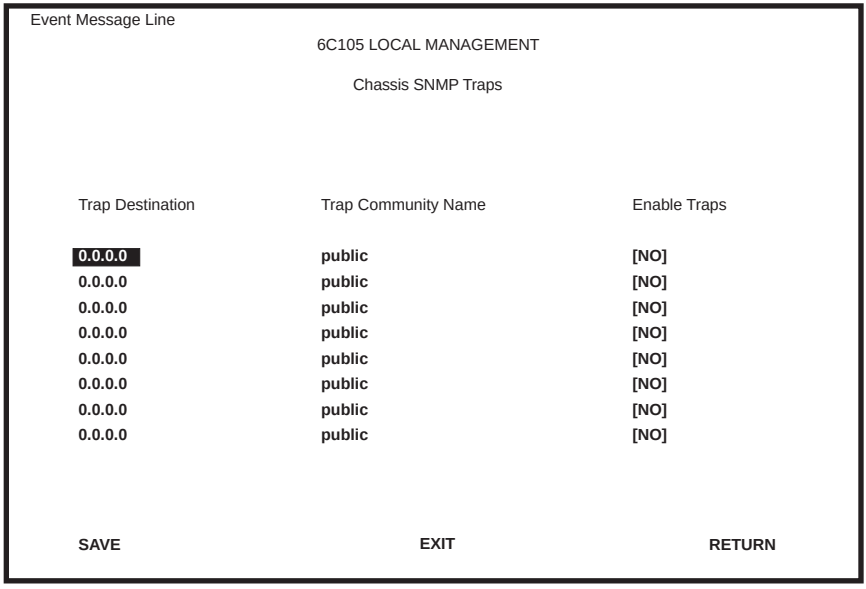


Figure 5-12 Chassis SNMP Traps Screen

The following explains each field of the SNMP Traps screen.

Trap Destination (Modifiable)
Indicates the IP address of the workstation to receive trap alarms. Up to eight different destinations can be defined.

Trap Community Name (Modifiable)
Displays the Community Name included in the trap message sent to the Network Management Station with the associated IP address.

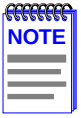
Enable Traps (Toggle)
Enables transmission of the traps to the network management station with the associated IP address. This field toggles between YES and NO.

5.9.1 Configuring the Trap Table

To configure the Trap table, proceed as follows:

1. Using the arrow keys, highlight the appropriate **Trap Destination** field.
2. Enter the IP Address of the workstation that is to receive traps. IP address entries must follow the DDN format.

   For example: 134.141.79.121
3. Press ENTER. If an invalid entry is entered “INVALID IP ENTERED” is displayed in the Event Message Line.
4. Using the arrow keys, highlight the **Trap Community Name** field. Enter the community name.
5. Press ENTER.
6. Using the arrow keys, highlight the **Enable Traps** field. Press the SPACE bar to choose either **YES** (send alarms from the chassis to the workstation), or **NO** (prevent alarms from being sent).
7. Using the arrow keys, highlight the **SAVE** command and press ENTER. The message “SAVED OK” displays on the screen.



Exiting without saving causes a “NOT SAVED?” message to appear. Edits will be lost if they are not saved before exiting.

The designated workstations now receive traps from the 6C105.

5.10 CHASSIS ENVIRONMENTAL SCREEN

The Chassis Environmental menu item allows the user to view chassis environmental information.

To access the Chassis Environmental Information screen from the Chassis Menu screen, use the arrow keys to highlight the **CHASSIS ENVIRONMENTAL** menu item and press ENTER. The Chassis Environmental Information screen, Figure 5-13, displays.

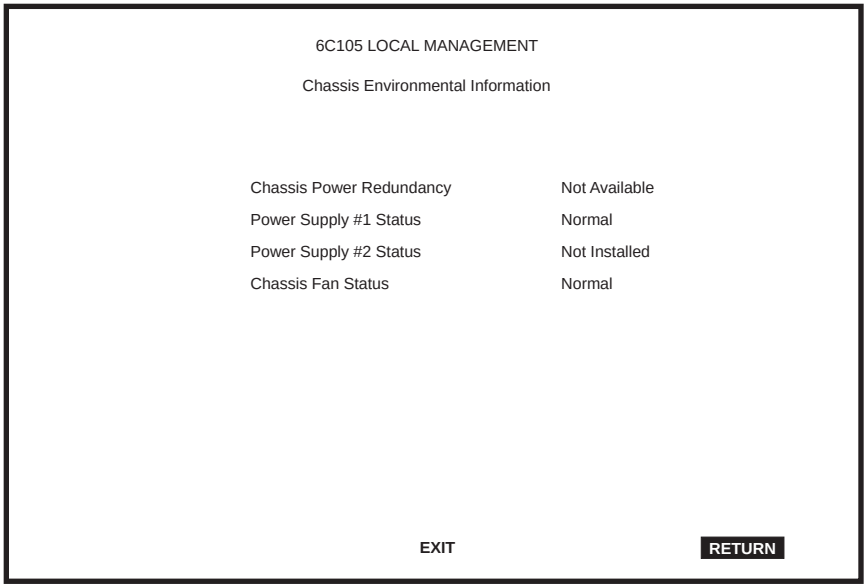


Figure 5-13 Chassis Environmental Information Screen

The following describes each of the Chassis Environmental Information screen fields.

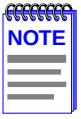
Chassis Power Redundancy (Read-Only)
Displays the current redundancy status of the 6C105 power supplies. This field will read either “Available” (there is power redundancy), or “Not Available” (there is no redundant power supply, or the one installed is defective).

Power Supply #*X* Status (Read-Only)
Displays the current status of power supplies 1 and 2 for the 6C105. This field will read either “Normal” (power redundancy is operating properly), “Fault” (power supply is defective), or “Not Installed” (no power supply in that slot).

Chassis Fan Status (Read-Only)
Displays the current status of the 6C105 fan tray. This field will read either “Normal” (fan tray is operating properly), “Fault” (fan tray is defective), or “Not Installed” (no fan tray installed-not a valid operating mode, see caution).

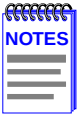
Operating a chassis without a fan tray installed may cause the chassis or installed modules to overheat and become a fire hazard. Cabletron Systems does not recommend operation of a chassis without a fully functioning fan tray unit.

5.11 PORT REDIRECT FUNCTION SCREEN



The Port Redirect Function screen may not be available depending on the operational mode that has been set for the chassis. Refer to your Release Notes to see what operational modes support the Port Redirect Function. Refer to Section 5.7.7, **Setting the Operational Mode**, for instructions on configuring the operational mode of all the modules installed in the chassis.

The Port Redirect Function screen, Figure 5-14, allows the user to set each one of the modules in the chassis (1 through 5), and the ports of the corresponding module installed, as a source or destination port. A port can be set to have one or more destination ports and chassis module slot numbers. For example, port 1 in module (slot) 1 can be set as a source port with three destinations, ports 2, 3, and 4 in module (slot) 3. Traffic from port 1 in module 1 is then automatically redirected to ports 2, 3, and 4 in module 3. Port 1 in module 1 can also serve as a destination port for other ports and modules. The port redirect function is extremely useful for troubleshooting purposes, as it allows traffic to be sent to a particular port(s) where, with the use of an analyzer or RMON probe, all current traffic from the source port(s) can be examined.



The module number corresponds to the slot number in which the module resides in the 6C105 chassis (1 through 5).

Although traffic from the source port (including, if desired, errored frames) is sent to the destination port, normal switching is still performed for all frames on the source port.

To access the Port Redirect Function screen from the Chassis Menu screen, use the arrow keys to highlight the **PORT REDIRECT FUNCTION** menu item and press ENTER. The Port Redirect Function screen, Figure 5-14, displays.

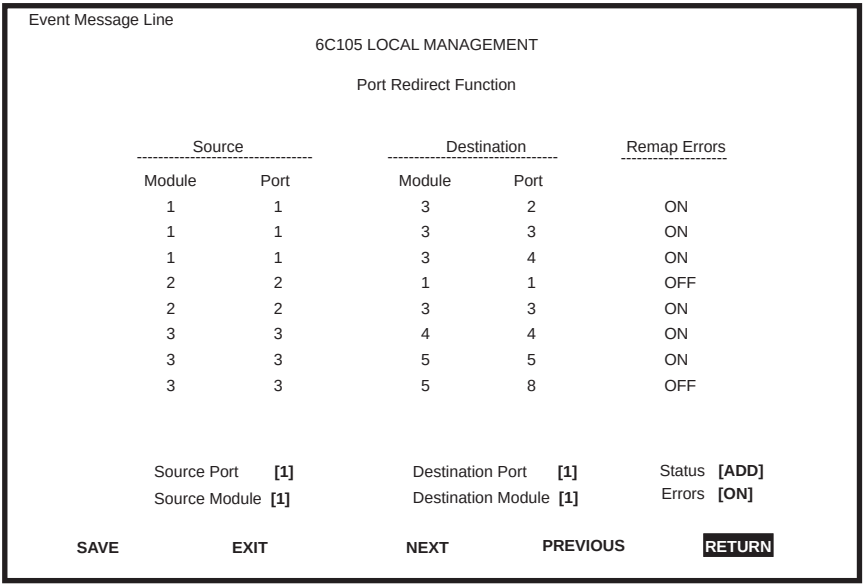


Figure 5-14 Port Redirect Function Screen

The following definitions briefly explain each field of the Port Redirect Function screen.

Source Module (Read-Only)
Displays which modules are currently set as source modules.

Source Port (Read-Only)
Displays which ports are currently set as source ports.

Destination Module (Read-Only)
Displays which modules are currently set as destination modules.

Destination Port (Read-Only)
Displays which ports are currently set as destination ports.

Remap Errors (Read-only)
Displays whether the corresponding source modules and ports are configured to send errored frames to the destination modules and ports, or to drop all errored frames before forwarding traffic.

Source Module [*n*] (Selectable)
Allows a selected module [*n*] to be configured as a source module.

Source Port [*n*] (Selectable)
Allows a selected port [*n*] to be configured as a source port.

Destination Module [*n*] (Selectable)
Allows a selected module [*n*] to be configured as a destination module.

Destination Port [*n*] (Selectable)
Allows a selected port [*n*] to be configured as a destination port.

Errors (Toggle)
Allows the user to configure the source modules and ports to either send errored frames to selected destination modules and ports (ON option), or to drop errored frames, and send only valid traffic to the destination modules and ports (OFF option). The default setting of this field is ON.

Status (Toggle)
Allows the user to add or delete the source/destination modules and ports selected in the Source/Destination Modules and ports fields.

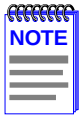
NEXT/PREVIOUS (Navigation Field)
There can be more than one Port Redirect Function screen depending on the number of port redirect entries. To get to the second or subsequent screens, use the arrow keys to highlight the NEXT field and press ENTER. The next screen of redirect entries displays. In the new screen, the navigation field PREVIOUS will display to allow the user to go back to the first or previous screens.

5.11.1 Changing Source and Destination Ports

Add or delete source/destination module and port entries as follows:

1. Use the arrow keys to highlight the **Source Module** field.
2. Press the SPACE bar or BACKSPACE one or more times to increment or decrement the module number displayed in the brackets [*n*] until the appropriate module number is displayed.

3. Use the arrow keys to highlight the **Source Port** field.
4. Press the SPACE bar or BACKSPACE one or more times to increment or decrement the port number displayed in the brackets [*n*] until the appropriate port number is displayed.
5. Use the arrow keys to highlight the **Destination Module** field.
6. Use the SPACE bar or BACKSPACE to step to the appropriate module number for the destination module.
7. Use the arrow keys to highlight the **Destination Port** field.
8. Use the SPACE bar or BACKSPACE to step to the appropriate port number for the destination port.
9. Use the arrow keys to highlight the **Errors** field.
10. Use the SPACE bar to select either the **ON** or **OFF** option and press ENTER. **ON** forces the source module and port to forward errored frames to the destination module(s) and port(s). **OFF** forces the errored frames to be dropped before forwarding traffic.
11. Use the arrow keys to highlight the **Status** field.
12. Use the SPACE bar to select either the **ADD** or **DEL** (delete) option. Press ENTER. This adds or deletes the selections made in steps 2 and 4 and also updates the screen Source Module, Source Port, Destination Module and Destination Port lists.



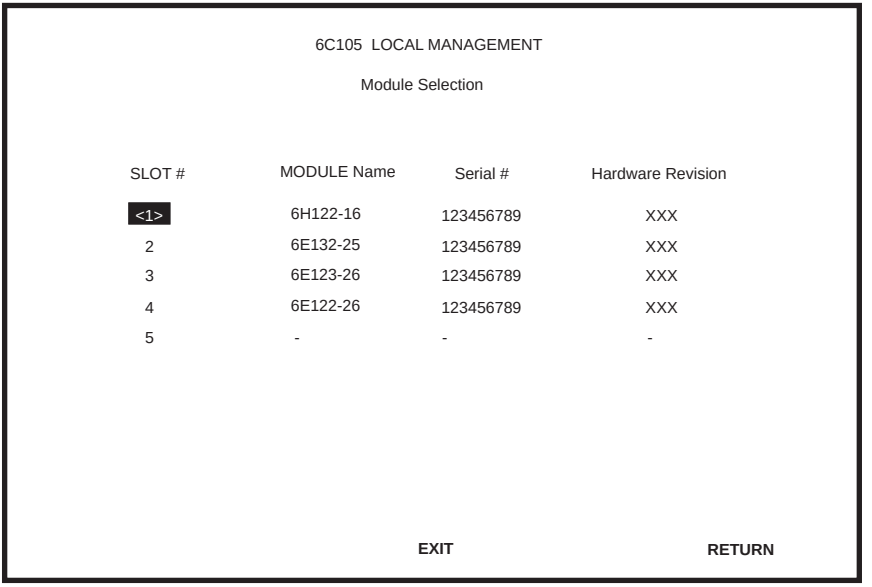
If more than one module and port is to be redirected, repeat steps 1 through 12 for each additional setting, then go to step 13 to save all the new settings at once.

13. Use the arrow keys to highlight **SAVE** at the bottom of the screen. Press ENTER. The message “SAVED OK” is displayed.

5.12 MODULE SELECTION SCREEN

The Module Selection screen is the access point to Local Management for all modules installed in the SmartSwitch 6000 chassis. By selecting a module, the Module Menu for the selected device displays. Figure 5-15 shows the Module Selection screen.

To access the Module Selection screen, use the arrow keys to highlight the **MODULES** menu item from the Main Menu screen and press ENTER. The Module Selection screen displays.



2361_39

Figure 5-15 Module Selection Screen

The following explains each Module Selection screen field as shown in Figure 5-15.

SLOT # (Selectable)

The Module # field displays the slot in which the module is installed. The module number enclosed in < > characters indicates the module to which the management terminal or Telnet session is connected.

MODULE Name (Read-only)
The Module Type field displays the type of interface module that is installed in each slot.

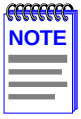
Serial # (Read-only)
Indicates the serial number of the module. The serial number is necessary when calling the Cabletron Systems Global Call Center concerning an issue with the device.

Hardware Revision (Read-only)
Reflects the hardware version of the module.

5.12.1 Selecting a Module

To select an individual module to perform Local Management functions, proceed as follows:

1. Use the arrow keys to highlight the desired module number in the SLOT # field.
2. Press ENTER, the applicable Module Menu screen displays. Proceed to Section 5.13.



When entering Local Management to a module by using a Telnet application, the display line at the top of the screen indicates how the module has been accessed. If the chassis IP address was used, the screen will display 6C105 LOCAL MANAGEMENT. If an IP address was assigned specifically for the module, and is used to Telnet to the module directly, then the display will read 6H122-16 LOCAL MANAGEMENT.

5.13 MODULE MENU SCREEN

The Module Menu screen is the access point for all Local Management screens for the 6H122-16. Figure 5-16 shows the 6H122-16 Module Menu screen.

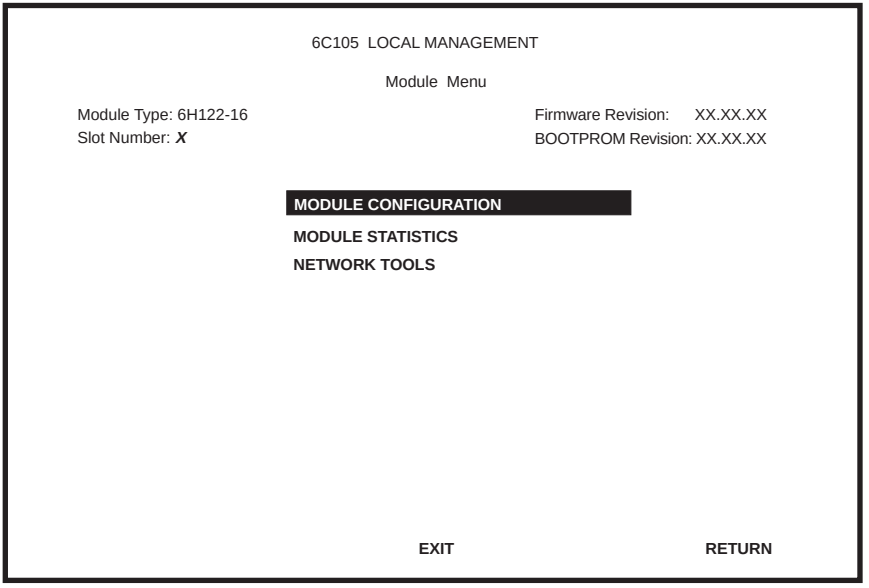


Figure 5-16 Module Menu Screen

The following explains each Module Menu screen field as shown in Figure 5-16:

MODULE CONFIGURATION

The Module Configuration screen provides access to the Local Management screens that are used to configure the 6H122-16 and also provides access to the Module Specific Configuration menu screen. This screen provides access to the screens that allow the user to check the 6H122-16 resources and set operating parameters specific to each port. For details about the Module Configuration Menu screen, refer to Section 5.14. For details about the Module Specific Configuration menu screen, refer to Section 5.20.

MODULE STATISTICS

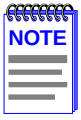
The Module Statistics screen provides statistics and performance information for the 6H122-16. For details about this screen, refer to Section 5.25.

NETWORK TOOLS

The Network Tools function resides on the 6H122-16 and consists of a series of commands that allow the user to access and manage network devices. Section 5.29 explains how to use the Network Tools utility.

5.14 MODULE CONFIGURATION MENU SCREEN

The Module Configuration Menu screen, Figure 5-17, provides access to Local Management screens that allow you to configure and monitor operating parameters, modify SNMP community names, set SNMP traps, configure switch parameters and configure 6H122-16 ports.



The following menu items on the Module Configuration Menu screen may not display if the operational mode of the module has been set to SECURE FAST VLAN:

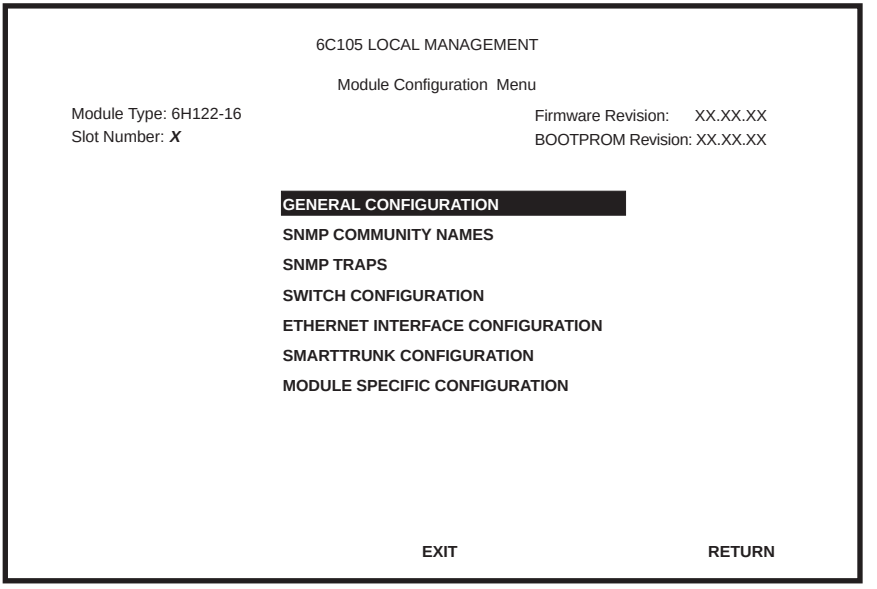
SWITCH CONFIGURATION

SMARTTRUNK CONFIGURATION

Refer to your Release Notes to see if the functionality provided by the above screens is supported in SECURE FAST VLAN mode.

Section 5.15.9 provides instructions on setting the operational mode.

To access the Module Configuration Menu screen from the Module Menu screen, use the arrow keys to highlight the **MODULE CONFIGURATION** menu item and press ENTER. The Module Configuration screen displays.



2361_15

Figure 5-17 Module Configuration Menu Screen

The following briefly explains each screen accessible from the Module Configuration Menu screen:

GENERAL CONFIGURATION

The General Configuration screen allows the user to monitor and configure operating parameters for the 6H122-16. For details, refer to Section 5.15.

SNMP COMMUNITY NAMES

The SNMP Community Names screen allows the user to enter new, change, or review the community names used as access passwords for Local/Remote management operation. Access is limited based on the password level of the user. For details, refer to Section 5.16.

SNMP TRAPS

The SNMP Traps screen provides display and configuration access to the table of IP addresses used for trap destinations and associated community names. For details, refer to Section 5.17.

SMARTTRUNK CONFIGURATION

The SmartTrunk Configuration screen allows the user to logically group interfaces together to create a greater bandwidth uplink. Refer to the Cabletron Systems *SmartTrunk User's Guide* for additional information.

ETHERNET INTERFACE CONFIGURATION

The Ethernet Interface Configuration screen indicates the link status, current and desired operational mode, and advertised ability for ports 1 through 16 on the 6H122-16. For details, refer to Section 5.19.

SMARTTRUNK CONFIGURATION

The SmartTrunk Configuration screen allows the user to logically group interfaces together to create wider bandwidth up links. Refer to the Cabletron Systems *SmartTrunk User's Guide* for additional information.

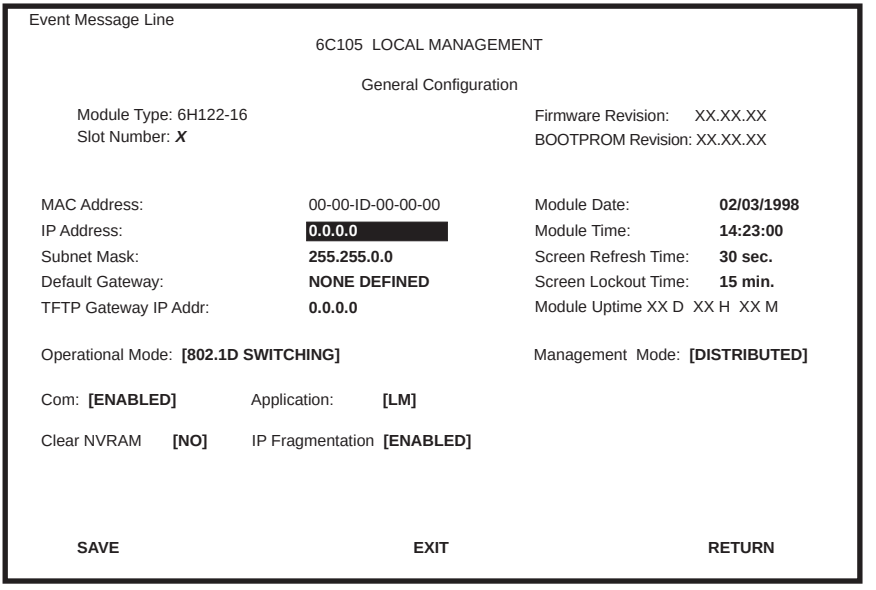
MODULE SPECIFIC CONFIGURATION

The Module Specific Configuration Menu screen allows the user to configure ports or check system resources specific to the 6H122-16. For details, refer to Section 5.20.

5.15 GENERAL CONFIGURATION SCREEN

The General Configuration screen, Figure 5-18, allows the user to set the system date and time, IP address and subnet mask, the default gateway, the TFTP Gateway IP address, the Operational Mode, the Management Mode, and the COM port configuration. The General Configuration screen also allows the user to Clear NVRAM, and enable or disable IP Fragmentation.

To access the General Configuration screen from the Module Configuration Menu screen, use the arrow keys to highlight the **GENERAL CONFIGURATION** menu item and press ENTER. The General Configuration screen displays.



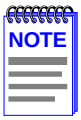
2361_16

Figure 5-18 General Configuration Screen

The following briefly explains each General Configuration screen field:

MAC Address (Read-Only)
Displays the base physical address of the module.

IP Address (Modifiable)
This field allows the IP address to be set for the 6H122-16. To set the IP address, refer to Section 5.15.1.



The IP Address can also be set through Runtime IP Address Discovery as previously described in Section 1.3.8.

Subnet Mask (Modifiable)
Displays the subnet mask for the module. A subnet mask "masks out" the network bits of the IP address by setting the bits in the mask to 1 when the network treats the corresponding bits in the IP address as part of the network or subnetwork address, or to 0 if the corresponding bit identifies the host. When an IP address is entered in the IP Address field, the Subnet Mask field automatically enters the default subnet mask for the IP address. For details about how to change the subnet mask from its default value, refer to Section 5.15.2.

Default Gateway (Modifiable)
Displays the default gateway for the 6H122-16. This field is not defined until an appropriate value is entered. For details about why and how to set the Default Gateway, refer to Section 5.15.3.

TFTP Gateway IP Addr (Modifiable)
Displays and allows the user to set the TFTP Gateway IP address for the 6H122-16. To set the TFTP Gateway IP address, refer to Section 5.15.4.

Module Date (Modifiable)
Contains a value that the module recognizes as the current date. To set a new module date, refer to Section 5.15.5.

Module Time (Modifiable)
Contains a value that the module recognizes as the current time. To enter a new time, refer to Section 5.15.6.

Screen Refresh Time (Modifiable)
Contains the rate at which the screens are updated. This setting determines how frequently (in seconds) information is updated on the screen. To enter a new update time, refer to Section 5.15.7.

Screen Lockout Time (Modifiable)
Contains the maximum number of minutes that the Local Management application displays a module's screen while awaiting input or action from a user. For example, if the number 5 is entered in this field, the user has up to five minutes to respond to each of the specified module's Local Management screens. In this example, after five minutes of "idleness" (no input or action), the terminal "beeps" five times, the Local Management application terminates the session, and the display returns to the Password screen. To enter a new lockout time, refer to Section 5.15.8.

Module Uptime (Read-Only)
Displays the total time that the module has been operating.

Operational Mode (Selectable)
This field sets the 6H122-16 to operate as an IEEE 802.1D switch (802.1D SWITCHING option), an IEEE 802.1Q switch (802.1Q SWITCHING option), or as a Cabletron Systems SecureFast switch (SECURE FAST VLAN option).

In 802.1D SWITCHING mode, the 16 ports located on the front panel are bridged to each other.

In 802.1Q SWITCHING mode, the 6H122-16 is able to increase its switching functionality by creating and maintaining IEEE port based VLANs.

When the operational mode is set to SECURE FAST VLAN, the 6H122-16 acts as a SecureFast switch. With the Cabletron Systems VLAN Manager software, the module is able to increase its switching functionality by creating and maintaining Virtual LANs (VLANs).

For details on how to select the Operational Mode, refer to Section 5.15.9.

Management Mode (Toggle)
This field toggles between DISTRIBUTED and STAND ALONE.

In DISTRIBUTED mode, Local Management is entered via the 6C105 password screen, and all chassis configuration screens are available to the user. All other modules installed in the chassis that are set for distributed management may also be accessed via a connection to a single COM port on one of the modules.

When using the IP address of the module to establish a remote connection (such as a Telnet or SNMP connection), the chassis LM screens will not be available. To access the chassis LM screens, the IP address of the chassis must be used to establish the connection.

In STAND ALONE mode, the module is isolated from the chassis configuration screens, and the module may not be accessed from a module that is in DISTRIBUTED mode. This provides additional security for any module to which the user may wish to restrict access. Section 5.15.10 describes how to set the Management Mode.

Com (Toggle)
This field allows the user to enable or disable the COM port. The selection toggles between ENABLED and DISABLED. The default is ENABLED. For details about setting up the COM port, refer to Section 5.15.11.

Application (Toggle)
Displays the application set for the COM port. This field allows you to set the application that the COM port will support, which includes the following:

- Local Management (LM) via a terminal or modem connection
- Uninterruptible Power Supply (UPS)

The UPS setting allows you to use the COM port to monitor an American Power Conversion Uninterruptible Power Supply (UPS). For the UPS, the baud rate is automatically set to 2400.

The baud rate setting for LM is automatically sensed.

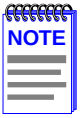
For details about how to configure the COM port for the various applications, refer to Section 5.15.11.

Clear NVRAM (Toggle)
This allows the user to reset NVRAM to the factory default settings. All user-entered parameters, such as IP address and Community Names are then replaced with 6H122-16 default configuration settings. For details, refer to Section 5.15.13.

IP Fragmentation (Toggle)
This field allows the user to enable or disable IP fragmentation. The default setting for this field is ENABLED. If the 6H122-16 will be bridged to an FDDI ring, IP Fragmentation should be enabled. If IP Fragmentation is disabled, all FDDI frames that exceed the maximum Ethernet frame size will be discarded. For details on enabling or disabling IP Fragmentation refer to Section 5.15.14.

5.15.1 Setting the IP Address

To set the IP address, perform the following steps:



If the 6C105 chassis has been assigned an IP address, it is not necessary to assign an IP address to the 6H122-16. All installed modules have the same IP address as the chassis. If a separate IP address for the module is desired, proceed as follows.

1. Use the arrow keys to highlight the **IP Address** field.
2. Enter the IP address into this field using Decimal Dotted Notation (DDN) format.

   For example: 134.141.79.120
3. Press ENTER. If the IP address is a valid format, the cursor returns to the beginning of the IP Address field. If the entry is not valid, the Event Message Line displays “INVALID IP ADDRESS OR FORMAT ENTERED”. Local Management does not alter the current value and refreshes the IP Address field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The warning screen shown in Figure 5-19 displays.

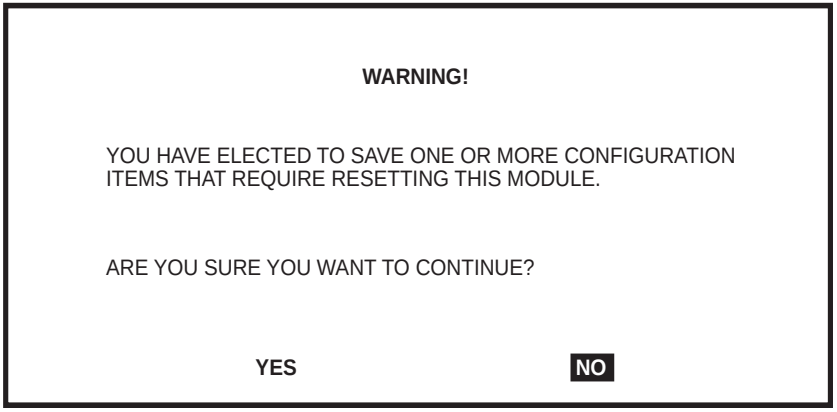


Figure 5-19 Configuration Warning Screen

5. Use the arrow keys to highlight the **YES** command. Press ENTER. The changes are saved and the module reboots.

5.15.2 Setting the Subnet Mask

If the management workstation that is to receive SNMP traps from the 6H122-16 is located on a separate subnet, the subnet mask for the 6H122-16 must be changed from its default.

To change the subnet mask from its default, perform the following steps:

1. Use the arrow keys to highlight the **Subnet Mask** field.
2. Enter the subnet mask into this field using Decimal Dotted Notation (DDN) format.

   For example: 255.255.255.0
3. Press ENTER. If the subnet mask is valid, the cursor returns to the beginning of the Subnet Mask field. If the entry is not valid, the Event Message Line displays “INVALID SUBNET MASK OR FORMAT ENTERED”. Local Management does not alter the current value, but it does refresh the Subnet Mask field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The warning screen shown in Figure 5-20 displays.

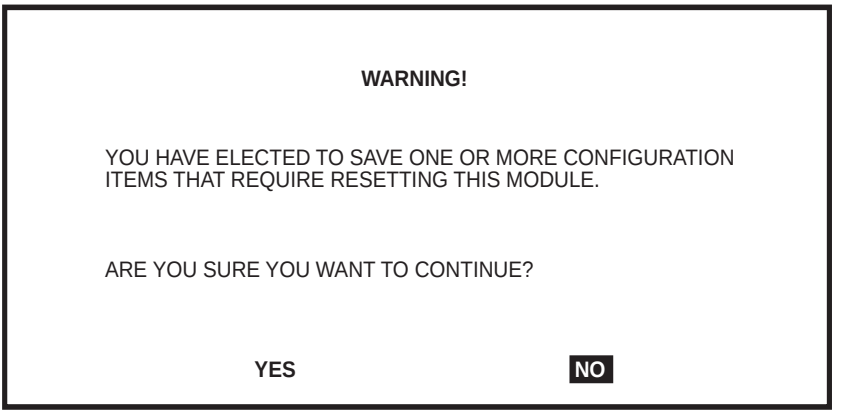


Figure 5-20 Configuration Warning Screen

5. Use the arrow keys to highlight the **YES** command and press ENTER. The changes are saved and the module reboots.

5.15.3 Setting the Default Gateway

If the SNMP management station is located on a different IP subnet than the 6H122-16, a default gateway must be specified. When an SNMP Trap is generated, the 6H122-16 sends the Trap to the default gateway. To set the default gateway, perform the following steps:

1. Use the arrow keys to highlight the **Default Gateway** field.
2. Enter the IP address of the default gateway using the DDN format.

   For example: 134.141.79.121
3. Press ENTER. If the default gateway entered is a valid format, the cursor returns to the beginning of the Default Gateway field. If the entry is not valid, the Event Message Line displays “INVALID DEFAULT GATEWAY OR FORMAT ENTERED”. Local Management does not alter the current value, but it does refresh the Default Gateway field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command.
5. Press ENTER. The Event Message Line at the top of the screen displays “SAVED OK”.

5.15.4 Setting the TFTP Gateway IP Address

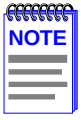
If the network TFTP server is located on a different IP subnet than the 6H122-16, a Gateway IP address should be specified. To set the TFTP Gateway IP address, perform the following steps:

1. Use the arrow keys to highlight the **TFTP Gateway IP Address** field.
2. Enter the IP address of the TFTP gateway using the DDN format.

   For example: 134.141.80.122
3. Press ENTER. If the TFTP gateway IP address entered is a valid format, the cursor returns to the beginning of the TFTP Gateway IP Address field. If the entry is not valid, the Event Message Line displays “INVALID TFTP GATEWAY IP ADDRESS OR FORMAT ENTERED”. Local Management does not alter the current value, but it does refresh the TFTP Gateway IP Address field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command.
5. Press ENTER. The Event Message Line at the top of the screen displays “SAVED OK”.

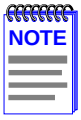
5.15.5 Setting the Module Date

The modules are year 2000 compliant, so the module date may be set beyond the year 1999. To set the module date, perform the following steps:



If the 6C105 chassis has been assigned a chassis date, it is not necessary to assign a module date to the 6H122-16. All installed modules recognize the chassis date of the 6C105.

1. Use the arrow keys to highlight the **Module Date** field.
2. Enter the date in this format: MM/DD/YYYY



It is not necessary to add separators between month, day, and year numbers as long as each entry has the correct number of characters. For example, to set the date to 01/17/1998, type “01171998” in the Module Date field.

3. Press ENTER to set the system calendar to the date in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

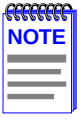
If the date entered is a valid format, the Event Message Line at the top of the screen displays “SAVED OK”. If the entry is not valid, Local Management does not alter the current value, but it does refresh the Module Date field with the previous value.

5.15.6 Setting the Module Time

To set the module clock, perform the following steps:

If the 6C105 chassis has been assigned a chassis time, it is not necessary to assign a module time to the 6H122-16. All installed modules recognize the chassis time of the 6C105.

1. Use the arrow keys to highlight the **Module Time** field.
2. Enter the time in 24-hour format: HH:MM:SS



When entering the time in the system time field, separators between hours, minutes, and seconds do not need to be added as long as each entry uses two numeric characters. For example, to set the time to 6:45 A.M., type “064500” in the Module Time field.

3. Press ENTER to set the system clock to the time in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is a valid format, the Event Message Line at the top of the screen displays “SAVED OK”. If the entry is not valid, Local Management does not alter the current value and refreshes the Module Time field with the previous value.

5.15.7 Entering a New Screen Refresh Time

The screen refresh time is set from 3 to 99 seconds with a default of 3 seconds. To set a new screen refresh time, perform the following steps:

1. Use the arrow keys to highlight the **Screen Refresh Time** field.
2. Enter a number from 3 to 99.
3. Press ENTER to set the refresh time to the time entered in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is within the 3 to 99 seconds range, the Event Message Line at the top of the screen displays “SAVED OK”. If the entry is not valid, the Event Message Line displays “PERMISSIBLE RANGE: 3...99” momentarily. Local Management does not alter the current setting, but it does refresh the Screen Refresh Time field with the previous value.

5.15.8 Setting the Screen Lockout Time

The screen lockout time can be set from 1 to 30 minutes with a default of 15 minutes. To set a new lockout time, perform the following steps:

1. Use the arrow keys to highlight the **Screen Lockout Time** field.
2. Enter a number from 1 to 30.
3. Press ENTER to set the lockout time in the input field.
4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the time entered is within the 1 to 30 minutes range, the Event Message Line at the top of the screen displays “SAVED OK”. If the entry is not valid, the Event Message Line displays “PERMISSIBLE RANGE: 1...30” momentarily. Local Management does not alter the current setting, but it does refresh the Screen Lockout Time field with the previous value.

5.15.9 Setting the Operational Mode

Before setting the operational mode, ensure that the items contained in this caution are fully understood.

If the module will be configured to operate as a SecureFast switch the following procedures should be performed before setting the operational mode:

The module must be assigned a unique IP address.

If the module will be a SecureFast switch, distributed management is not allowed. The Management Mode of the module will automatically be set to STANDALONE. The Management Mode field will no longer display on the General Configuration screen, and the module will no longer support Chassis configuration and Module selection screens.

The module has been assigned SNMP community names from the module SNMP Community Names screen (Section 5.16). In Standalone management mode, the module does not use the community names of the 6C105 chassis.

To set the Operational Mode, proceed as follows:

1. Use arrow keys to highlight the **Operational Mode** field.
2. Press the SPACE bar to step to the appropriate operation mode (**802.1D SWITCHING**, **802.1Q SWITCHING**, or **SECURE FAST VLAN**).
3. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The warning screen shown in Figure 5-21 displays.

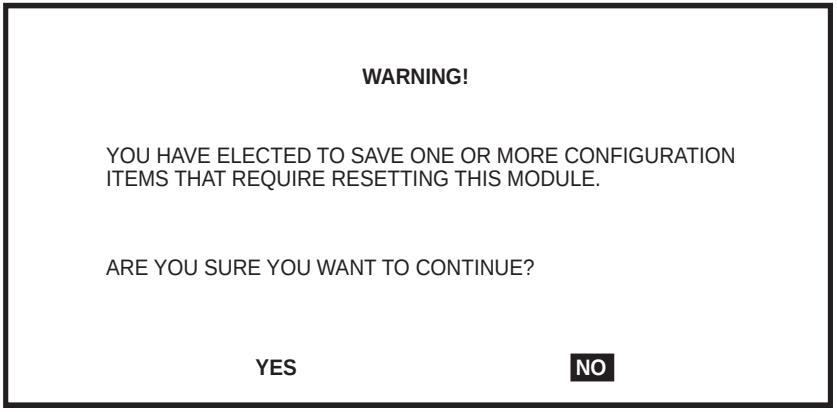
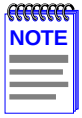


Figure 5-21 Configuration Warning Screen

4. Use the arrow keys to highlight the **YES** command and press ENTER. The changes are saved and the module reboots.



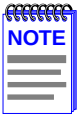
Upon saving the new operational mode, the module will reboot.

If the 6H122-16 has been set to **802.1Q SWITCHING**, refer to your *Port Based VLAN User's Guide* to configure the module for this type of operation.

If the 6H122-16 has been set to **SECURE FAST VLAN**, refer to your SecureFast documentation set to configure the module for this type of operation.

5.15.10 Setting the Management Mode

To set the management mode, perform the following steps:



Upon saving the new Management Mode, the module will reboot.
If the module will be set to STANDALONE, ensure the following procedures have been completed:

The module has been assigned a unique IP address.

The module has been assigned SNMP community names from the module SNMP Community Names screen (Section 5.16). In STAND ALONE management mode, the module does not use the community names of the 6C105 chassis.

1. Use the arrow keys to highlight the **Management Mode** field:
2. Use the SPACE bar to toggle the options (**DISTRIBUTED** or **STAND ALONE**) until the desired mode displays.
3. Use the arrow keys to highlight the **SAVE** command, then press ENTER. The warning screen shown in Figure 5-22 displays.

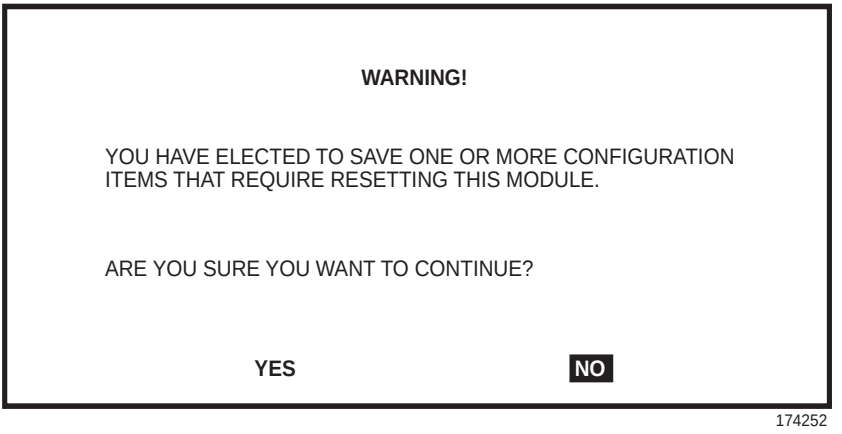


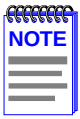
Figure 5-22 Configuration Warning Screen

4. Use the arrow keys to highlight the **YES** command and press ENTER. The changes are saved and the module reboots.

5.15.11 Configuring the COM Port

Before altering the COM port settings, ensure that a valid IP address is set for the module or chassis. (Refer to Section 5.15.1, **Setting the IP Address**). Read this entire COM port configuration section before changing the settings of the COM port.

The 6H122-16 COM port supports the following applications:



Refer to the Release Notes included with the 6H122-16 to verify which COM Port applications are currently supported.

- Local Management connections
- American Power Conversion Uninterruptible Power Supply (UPS) connections

To configure the COM port, proceed as follows:

1. Use the arrow keys to highlight the **Com** field.

Do **NOT** disable or alter the settings of the COM port while operating the current Local Management connection through a terminal. Altering the COM port settings disconnects the Local Management terminal from the port, and ends the Local Management session. If the module was previously assigned a valid IP address, reenter Local Management by establishing a Telnet connection to the module. If the module does not have a valid IP address and the COM port has been disabled or the settings changed, reset NVRAM on the module (refer to Section B.2) to reestablish COM port communications.

2. Press the SPACE bar to choose either **ENABLED** or **DISABLED**. The COM port must be **ENABLED** if it will be used for Local Management or UPS applications. Select **DISABLED** if you wish to disable the COM port for additional module security.

If the COM port is reconfigured without a valid IP address set on the module or chassis, the message shown in Figure 5-23 displays. Do not continue unless the outcome of the action is fully understood.

Figure 5-23 COM Port Warning Screen

NOTE

If the 6C105 chassis has been configured with a valid IP address this screen will not appear. When the chassis is assigned a valid IP address all the interface modules installed share this same address.

3. Use the arrow keys to highlight **YES**. Press ENTER.
4. If you **ENABLED** the port, proceed to Section 5.15.12. If you **DISABLED** the port, use the arrow keys to highlight **SAVE** at the bottom of the screen, then press ENTER. When the message "SAVED OK" displays, the edits are saved.

CAUTION

Exiting without saving causes the message "NOT SAVED -- PRESS SAVE TO KEEP CHANGES" to appear. Exiting without saving causes all edits to be lost.

5.15.12 Changing the Com Port Application

After enabling the COM port as described in Section 5.15.11, you can select one of the applications supported by the COM port: LM, and UPS. The default application is LM.

To change the COM port application:

1. Use the arrows keys to highlight the **Application** field.
2. Use the SPACE bar or BACKSPACE to step through the available settings until the operation you require appears. Table 5-3 lists the available settings and their corresponding applications.

Table 5-3. COM Port Application Settings

Setting	Application
LM	Local Management Session
UPS	APC Power Supply SNMP Proxy

3. Press ENTER to accept the application.
4. Use the arrow keys to highlight **SAVE** at the bottom of the screen, then press the ENTER key.
5. When the message “SAVED OK” appears, the edits you made are saved.

When the COM port is configured to perform the UPS application, all future Local Management connections must be made by establishing a Telnet connection to the module. Ensure that the module has a valid IP address before saving changes to the COM port application. If the module does not have a valid IP address and the changes are saved, refer to Appendix B for instructions on clearing NVRAM in order to reestablish COM port communications.

5.15.13 Clearing NVRAM

Clearing NVRAM will result in the loss of all user-entered parameters. Do not proceed unless this procedure is completely understood.

Clearing NVRAM allows the user to clear all user-entered parameters, such as IP address and Community Names from NVRAM.

Clear NVRAM as follows:

1. Use the arrow keys to highlight the **Clear NVRAM** field.
2. Use the SPACE bar to toggle the field to **YES**.
3. Use the arrow keys to highlight **SAVE** at the bottom of the screen.
4. Press ENTER. The warning shown in Figure 5-24 displays.

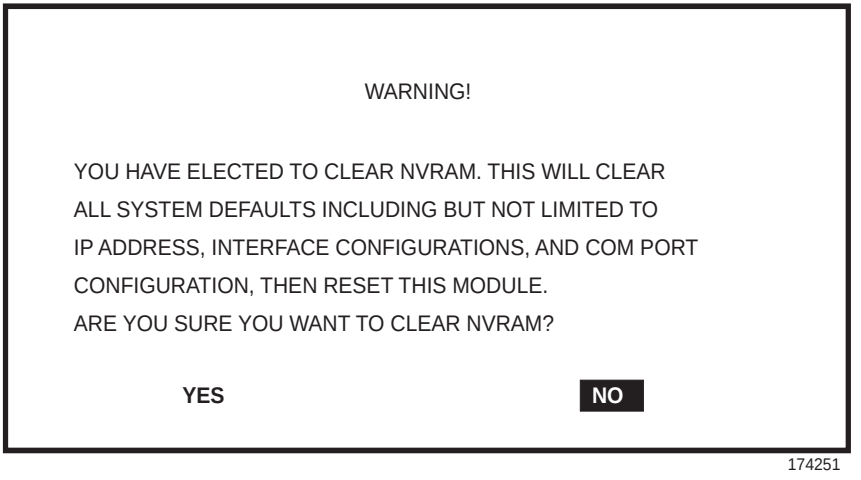


Figure 5-24 Clear NVRAM Warning Screen

5. To clear NVRAM, use the arrow keys to highlight **YES** and press ENTER. The message “CLEARING NVRAM. REBOOT IN PROGRESS...” displays.

The 6H122-16 clears NVRAM and reboots. All user-entered parameters default to factory settings.

5.15.14 Enabling/Disabling IP Fragmentation

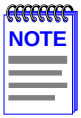
To enable or disable IP fragmentation, proceed as follows:

If the 6H122-16 is being bridged to an FDDI ring IP Fragmentation should be enabled. If IP Fragmentation is disabled, all FDDI frames that exceed the maximum Ethernet frame size will be discarded.

1. Use the arrow keys to highlight the **IP Fragmentation** field.
2. Press the SPACE bar to choose either **ENABLED** or **DISABLED**.
3. Use the arrow keys to highlight the **SAVE** command.
4. Press ENTER. The Event Message Line at the top of the screen displays “SAVED OK”.

5.16 SNMP COMMUNITY NAMES SCREEN

The SNMP Community Names menu item allows the user to set Local/Remote Management community names. Community names act as passwords to Local/Remote Management and are agents of security access to the 6H122-16. Access to the 6H122-16 is controlled by invoking any of three different levels of security authorization (read-only, read-write, and super-user).



If the 6C105 has been assigned community names, it is not necessary to assign community names to the individual modules installed in the chassis unless the user wishes to limit access to 6C105 chassis screens by assigning different community names to the module. When this is done access is limited to the screens specific to the module the terminal is attached to and the CHASSIS menu item of the Main Menu screen will not appear.

Super-User access gives the user full management privileges, allows existing passwords to be changed, as well as all modifiable MIB objects.

To access the SNMP Community Names screen from the Module Configuration Menu screen, use the arrow keys to highlight the **SNMP COMMUNITY NAMES** menu item and press ENTER. The SNMP Community Names screen, Figure 5-25, displays.

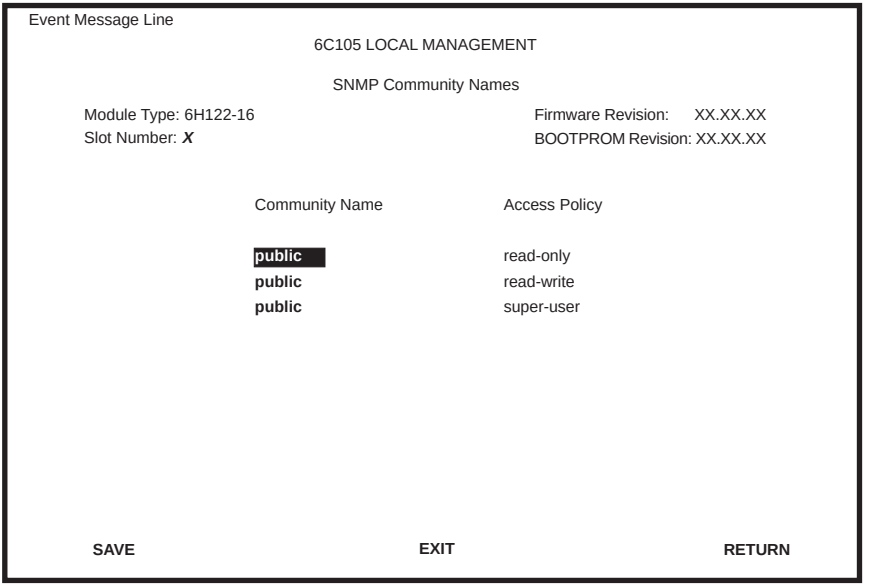


Figure 5-25 SNMP Community Names Screen

The following explains each SNMP Community Names screen field:

Community Name (Modifiable)
Displays the user-defined name through which a user accesses 6H122-16 management. Any community name assigned here acts as a password to Local/Remote Management.

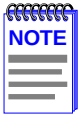
Access Policy (Read-Only)
Indicates the access accorded each community name. Possible selections are as follows:

read-only	This community name allows read-only access to the 6H122-16 MIB objects, and excludes access to security-protected fields of read-write or super-user authorization.
read-write	This community name allows read and write access to the 6H122-16 MIB objects, excluding security protected fields for super-user access only.

super-user	This community name permits read-write access to the 6H122-16 MIB objects and allows the user to change all modifiable parameters including community names, IP addresses, traps, and SNMP objects.

5.16.1 Establishing Community Names

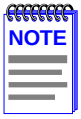
The password used to access Local Management at the Password Screen must have Super-User access in order to view and edit the SNMP Community Names screen. Using a password with read-only or read-write access does not allow the user to view or edit the SNMP Community Names screen.



Any community name assigned in the SNMP Community Names screen is a password to its corresponding level of access to Local/Remote Management. The community name assigned Super-User access is the only one that gives the user complete access to Local/Remote Management.

To establish community names, proceed as follows:

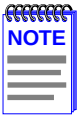
1. Use the arrow keys to highlight the **Community Name** field adjacent to the selected access level.
2. Enter the password in the field (maximum 31 characters).
3. Press ENTER.
4. Repeat steps 1 through 3 to modify the other community names.
5. Use the arrow keys to highlight **SAVE** at the bottom of the screen and press ENTER. The message “SAVED OK” displays. The community names are saved to memory and their access modes implemented.



Exiting without saving causes a “NOT SAVED?” message to display at the top left of the screen. Edits will be lost if they are not saved before exiting.

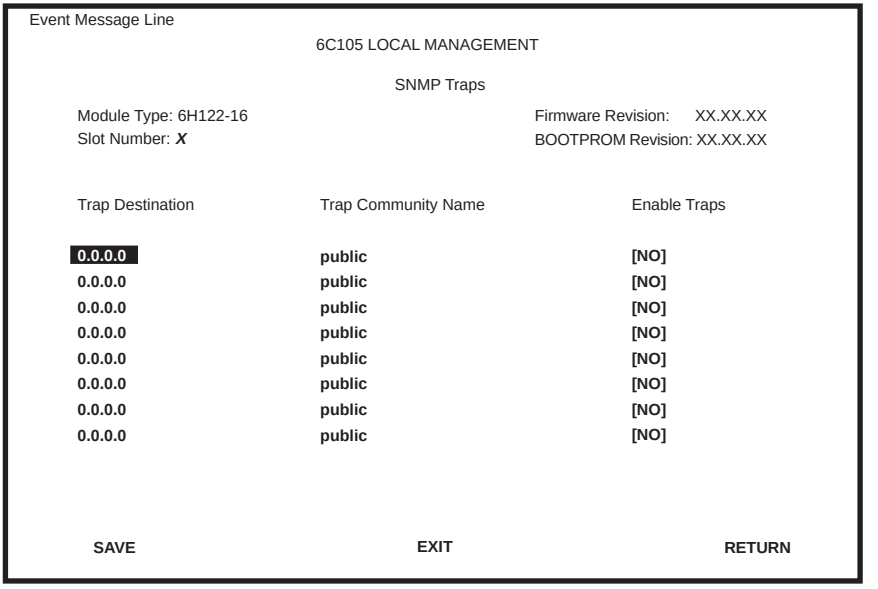
5.17 SNMP TRAPS SCREEN

Since the 6H122-16 is an SNMP compliant device, it can send messages to multiple Network Management Stations to alert users of status changes. The SNMP Traps screen is shown in Figure 5-26.



It is only necessary to assign SNMP traps if the user desires the traps to be sent to different addresses than those assigned in Section 5.8 which details how to set SNMP Traps for the 6C105 chassis.

To access the SNMP Traps screen from the Module Configuration Menu screen, using the arrow keys to highlight the **SNMP TRAPS** menu item and press ENTER. The SNMP Traps screen displays.



2361_17a

Figure 5-26 SNMP Traps Screen

The following explains each field of the SNMP Traps screen.

Trap Destination (Modifiable)
Indicates the IP address of the workstation to receive trap alarms. Up to eight different destinations can be defined.

Trap Community Name (Modifiable)
Displays the Community Name included in the trap message sent to the Network Management Station with the associated IP address.

Enable Traps (Toggle)
Enables transmission of the traps to the network management station with the associated IP address. This field toggles between YES and NO.

5.17.1 Configuring the Trap Table

To configure the Trap Table, proceed as follows:

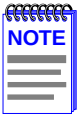
1. Using the arrow keys, highlight the appropriate **Trap Destination** field.
2. Enter the IP Address of the workstation that is to receive traps. IP address entries must follow the DDN format.

   For example: 134.141.79.121
3. Press ENTER. If an invalid entry is entered “INVALID IP ENTERED” is displayed in the Event Message Line.
4. Using the arrow keys, highlight the **Trap Community Name** field. Enter the community name.
5. Press ENTER.
6. Using the arrow keys, highlight the **Enable Traps** field. Press the SPACE bar to choose either **YES** (send alarms from the module to the workstation), or **NO** (prevent alarms from being sent).
7. Using the arrow keys, highlight the **SAVE** command and press ENTER. The message “SAVED OK” displays on the screen.

The designated workstations now receive traps from the 6H122-16.

5.18 SWITCH CONFIGURATION SCREEN

The Switch Configuration screen, Figure 5-27, provides the basic setup options to modify switch operations in your network.



The Switch Configuration screen will not be available if the operational mode of the module has been set to SECURE FAST VLAN. This screen may only be used by modules configured to operate as 802.1D or 802.1Q switches.

To access the Switch Configuration screen from the Module Configuration Menu screen, use the arrow keys to highlight the **SWITCH CONFIGURATION** menu item and press ENTER. The Switch Configuration screen, Figure 5-27, displays ports 1 through 8. To view or edit the fields for ports 9 to 16, highlight the navigation field **[9-16]** at the bottom of the screen and press the ENTER key. Once in the screen viewing ports 9 to 16, the navigation fields [1-8] and [17-21] can be seen. These fields can be used to go to the first screen and last screen, respectively.

Event Message Line

6C105 LOCAL MANAGEMENT

Switch Configuration

Module Type: 6H122-16
Slot Number: *X*

Firmware Revision: XX.XX.XX
BOOTPROM Revision: XX.XX.XX

Switch Address: 00-00-1D-00-00-00
Number of Ports: 21

Type of STA: **[IEEE]**
Age Time (sec): **300**

Port #	MAC Address	State	Status
1	00-00-1D-00-00-00	learning	**[ENABLED]**
2	00-00-1D-00-00-01	disabled	**[DISABLED]**
3	00-00-1D-00-00-02	standby	**[ENABLED]**
4	00-00-1D-00-00-03	disabled	**[DISABLED]**
5	00-00-1D-00-00-04	listening	**[ENABLED]**
6	00-00-1D-00-00-05	disabled	**[DISABLED]**
7	00-00-1D-00-00-06	forwarding	**[ENABLED]**
8	00-00-1D-00-00-07	forwarding	**[ENABLED]**

SAVE **[9-16]** **EXIT** **RETURN**

2361_18

Figure 5-27 Switch Configuration Screen

Ports 17 through 20 represent the backplane connections that the 6H122-16 has with the 6C105 chassis. The module has a direct connection to every other slot in the chassis.

The following describe each field of the Switch Configuration screen:

Switch Address (Read-Only)
Displays the base MAC address of the switch.

Number of Ports (Read-Only)
Displays the total number of switched ports on the module.

Type of STA (Selectable)
Allows the user to set the method that switches use to decide which switch is the controlling (Root) switch when two or more switches exist in parallel (Spanning Tree Algorithm [STA]). Valid entries include IEEE, DEC, and NONE. To set the STA, refer to Section 5.18.1.

Age Time (Modifiable)
Allows the user to set the amount of time (in seconds) the 6H122-16 will keep an address in its switch table before discarding it. The module will discard an address from its switch table if it does not receive a valid frame from the applicable address in the amount of time specified in the Age Time field. To change the Age Time field from the default value of 300 seconds, refer to Section 5.18.2.

Port # (Read-Only)
Lists each switch port on the module. If the number of ports is greater than eight, then the additional ports are listed on subsequent screens.

MAC Address (Read-Only)
Displays the hardware address assigned to each listed port.

State (Read-Only)
Disabled: Management disabled this interface. No traffic is received or forwarded while the interface is disabled.

Listening: The switch is not adding information to the Transparent Database. The switch is monitoring BPDU traffic while preparing to move from the learning to the forwarding state.

Learning: The switch is learning the network address of this interface. The switch enters the learning state when the Transparent Database is created (during start-up or after being deleted), or when the Spanning Tree Algorithm detects a network topology change.

Forwarding: The switch is on line and this interface is forwarding traffic.

Blocking: This interface will not forward any traffic through the switch because a loop condition has been detected by the STA.

Status (Toggle)
Allows the user to disable or enable a port by setting the status of the listed interface to either ENABLED or DISABLED. To set the port status, refer to Section 5.18.3.

[1-8], [9-16], [17-21] (Navigation Field)
The Switch Configuration screen can only show the configuration for eight ports at a time. When the specific Navigation field is available, it allows the user to view the Switch Configuration for ports 1 through 8, ports 9 through 16, or ports 17 through 21. Once this field is highlighted, press the ENTER key to go to the desired screen.

5.18.1 Setting the STA

The Spanning Tree Algorithm (STA) setting allows the user to set the method that the switches use to decide which is the controller (Root) switch when two or more switches are in parallel. The available selections are **IEEE**, **DEC**, and **NONE**.

To set the STA, proceed as follows:

1. Use the arrow keys to highlight the **Type of STA** field.
2. Use the SPACE bar to step to the appropriate setting (**IEEE**, **DEC**, or **NONE**).
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” is displayed.

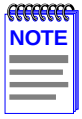
5.18.2 Setting the Age Time

To set the Age Time, proceed as follows:

1. Use the arrow keys to highlight the **Age Time** field.
2. Enter the desired Age Time in increments of 10. The available Age Time range is 10 to 1,000,000 seconds with the default value being 300 seconds.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” is displayed.

5.18.3 Setting (Enabling or Disabling) the Port Status

To set the status of an interface (port), proceed as follows:



Disabling the port status of a backplane connection will block the module from passing user traffic to the applicable module slot in the 6C105 chassis. SNMP and other management traffic (e.g., ping and Telnet traffic), however, will still pass via the backplane to the applicable module slot.

1. Use the arrow keys to highlight the **Status** field of the port.
2. Use the SPACE bar to toggle to either **ENABLED** or **DISABLED**.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” is displayed.

5.19 ETHERNET INTERFACE CONFIGURATION

To access the Ethernet Interface Configuration screen from the Module Configuration Menu screen, use the arrow keys to highlight the **ETHERNET INTERFACE CONFIGURATION** menu item and press ENTER. The Ethernet Interface Configuration screen displays.

Event Message Line

6C105 LOCAL MANAGEMENT

Ethernet Interface Configuration

Module Type: 6H122-16
Slot Number: ***X***

Firmware Revision: XX.XX.XX
BOOTPROM Revision: XX.XX.XX

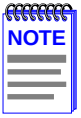
Port Num	Port Type	Link Status	Current Oper. Mode	Desired Oper. Mode	Advertised Ability	
1	FE-100TX	Link	100Base-TX	**[Auto-Neg]**	**[100Base-TX]**	**[Disabled]**
2	FE-100TX	Link	10Base-TFD	**[100Base-TX]**	**[100Base-TX]**	**[Enabled]**
3	FE-100TX	No Link	100Base-TX	**[100Base-TX]**	**[100Base-TX]**	**[Enabled]**
4	FE-100TX	Link	100Base-TX	**[100Base-TX]**	**[100Base-TX]**	**[Enabled]**
5	FE-100TX	Link	100Base-TX	**[100Base-TX]**	**[100Base-TX]**	**[Disabled]**
6	FE-100TX	No Link	10Base-T	**[100Base-TX]**	**[100Base-TX]**	**[Enabled]**
7	FE-100TX	Link	100Base-TX	**[100Base-TX]**	**N/A**	
8	FE-100TX	No Link	Unknown	**[Auto-Neg]**	**[10Base-TFD]**	**[Enabled]**

Flow Control Admin Status: **[Disabled]**

SAVE **[9-16]** **EXIT** **RETURN**

2361_23

Figure 5-28 Ethernet Interface Configuration Screen for the 6H122-16



All ports are capable of 10 or 100 Mbps operation, however only ports 15 and 16 support Full Duplex Switched Ethernet (FDSE) for 100 Mbps.

Ports 15 and 16 auto-negotiate to 100BASE-TXFD by default and can also be manually set to 100BASE-TXFD, but ports 1 through 14 cannot be set to nor auto-negotiate to 100BASE-TXFD.

All ports can be set and auto-negotiate to 10BASE-TXFD.

The following section briefly explains each field of the Ethernet Interface Configuration screen:

Port Num (Read-Only)
Displays the number of the front panel interface.

Port Type (Read-Only)
Displays the name of the interface installed in ports 1 through 16. All ports are identified as FE-100TX.

Link Status (Read-Only)
Indicates whether or not there is a physical connection from a particular port to another 10BASE-T, 100BASE-TX, or 100BASE-TXFD device. One of the following values is displayed:

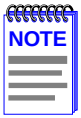
- Link – There is a link signal present and a valid physical connection to another 10BASE-T, 100BASE-TX, or 100BASE-TXFD device.
- No Link – There is no link signal present and there is no valid physical connection to another device.

Current Oper. Mode (Read-only)
This field displays the current operating mode of a port. Depending on the connection negotiated, this field displays the following:

100Base-TX interface – Auto-Neg, Unknown (if there is no Link), 10Base-T, 10Base-TFD (full duplex), 100Base-TX, or 100Base-TXFD (full duplex, ports 15 and 16 only).

Desired Oper. Mode (Selectable)
This field allows the user to select the desired operational mode for an interface.

FE-100TX Interface – The field steps between Auto-Neg, 10Base-T, 10Base-TFD (full duplex), 100Base-TX, and 100Base-TXFD (full duplex, ports 15 and 16 only). In normal operation, the port with an FE-100TX interface is capable of auto-negotiating the operational mode and no further user setup is required. For details on how to set the Operational Mode, refer to Section 5.19.2.



In normal operation, ports 1 through 16 automatically establish a link with the device at the other end of the segment without requiring user setup. However, Local Management provides the user with the option of manually configuring that port.

Advertised Ability (Selectable)
During auto-negotiation, the port "tells" the device at the other end of the segment what its capabilities are. The capabilities of a port are 10BASE-T, 10BASE-TFD (full duplex mode), 100BASE-TX and 100BASE-TXFD (full duplex mode, ports 15 and 16 only). In normal operation, with all capabilities enabled, the port "advertises" that it has the ability to operate in any mode. The Network Manager may choose to set up the port so that only a portion of the available capabilities are advertised and the others are disabled. For example, only 100BASE-TX and 100BASE-TXFD (ports 15 and 16 only) might be enabled so that only devices that operate at 100 Mbps can communicate with that port. Section 5.19.3 describes how to enable or disable advertised modes.

Flow Control Admin Status (Selectable)
Enabling this setting controls whether or not the switch will block traffic on all ports when there is excessive traffic for the switch to process. This will clear the ports and allow the switch to process the current frame information. Section 5.19.4 explains how to enable or disable this option.

5.19.1 Configuring the Ports

In normal operation, a 6H122-16 interface automatically establishes a link with the device at the other end of the segment and no user setup is required. Section 5.19.2 and Section 5.19.3 provide instructions for manually configuring the interface.

5.19.2 Setting the Operational Mode

Use this field to set the active technology. This field steps between Auto-Negotiation, 10BASE-T, 10BASE-TFD (full duplex), 100BASE-TX, and 100BASE-TXFD (full duplex, ports 15 and 16 only). If Auto-Negotiation is selected, the port automatically sets the active technology. To manually set the active technology through Local Management, proceed as follows:

1. Use the arrow keys to highlight the **Desired Oper. Mode** field.
2. Use the SPACE bar to select the desired mode. Press ENTER. If any mode other than auto-negotiation is selected, the port only operates in the chosen mode and auto-negotiation is disabled.

3. Use the arrow keys to highlight the **SAVE** command. Press ENTER. The message "SAVED OK" displays and Local Management saves the changes to memory. The selected mode is displayed in both the Desired Operational Mode field and the Current Operational Mode field.

5.19.3 Setting the Advertised Ability

During normal operation, ports 1 through 16 auto-negotiate to the highest speed possible. Under some circumstances, the Network Administrator may want the port to advertise only some of the available modes and not operate in other modes. This field steps between 10BASE-T, 10BASE-TFD (full duplex), 100BASE-TX, and 100BASE-TXFD (ports 15 and 16 only).

To set the advertised ability, proceed as follows:

1. Use the arrow keys to highlight the **Advertised Ability** field.
2. Use the SPACE bar to select the desired mode.
3. Use the RIGHT-ARROW key to move across to the **Enabled/Disabled** field to the right of the selection.
4. Use the SPACE bar to select **Enabled** or **Disabled**. Press ENTER. Continue this process until you have completed enabling or disabling the advertised modes.
5. Use the arrow keys to highlight the **SAVE** command. Press ENTER. The message "SAVED OK" displays and Local Management saves the changes to memory.

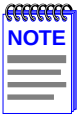
5.19.4 Setting the Flow Control Admin Status

This field toggles between ENABLED and DISABLED. To enable or disable Flow Control, do the following:

1. Use the arrow keys to highlight the **Flow Control Admin Status** field.
2. Use the SPACE bar to toggle the field to the desired setting. Press ENTER.
3. Use the arrow keys to highlight the **SAVE** command. Press ENTER. The message "SAVED OK" displays and Local Management saves the changes to memory. The selected mode is displayed in the field.

5.20 MODULE SPECIFIC CONFIGURATION MENU SCREEN

The Module Specific Configuration menu screen, Figure 5-29, allows the user to select one of up to five screens to configure ports or check system resources specific to the 6H122-16.



The BROADCAST SUPPRESSION menu item on the Module Specific Configuration menu screen may not display if the operational mode of the module has been set to SECURE FAST VLAN. The PORT REDIRECT menu item may not display if the operational mode of the module has been set to 802.1Q.

Refer to your Release Notes to see if the functionality provided by the above screens is supported.

Section 5.15.9 provides instructions on setting the operational mode.

To access the Module Specific Configuration menu screen from the Module Configuration Menu screen, use the arrow keys to highlight the **MODULE SPECIFIC CONFIGURATION** menu item and press ENTER. The Module Specific Configuration menu screen displays.

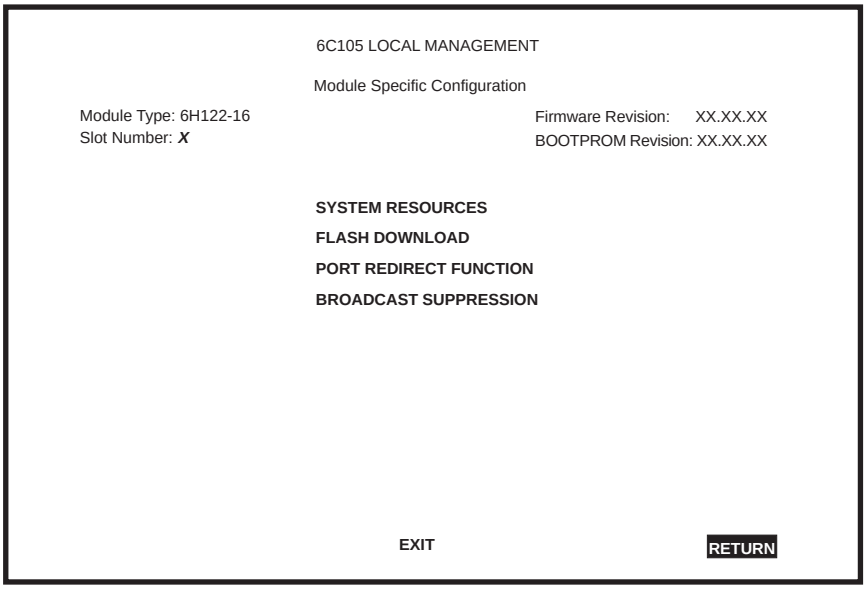


Figure 5-29 Module Specific Configuration Screen

The following explains each field of the Module Specific Configuration menu screen:

SYSTEM RESOURCES

The System Resources screen displays the amount of FLASH memory, DRAM, and NVRAM installed, details how much memory is available and provides information on 6H122-16 operation. For details, refer to Section 5.21.

FLASH DOWNLOAD

The FLASH Download screen allows the user to force the 6H122-16 to download a new image file to FLASH memory from a TFTP server. For details, refer to Section 5.22.

PORT REDIRECT FUNCTION

The Port Redirect Function screen allows the user to redirect traffic from one or more ports on the module to a specific destination port on the module. For details, refer to Section 5.23.

BROADCAST SUPPRESSION

The Broadcast Suppression screen allows the user to set a desired limit of receive broadcast frames per port per second. For details, refer to Section 5.24.

802.1Q VLAN CONFIGURATION

This menu item will only display if the module has been configured to operate as an IEEE 802.1Q switch. When selected, this menu item opens the VLAN Main Menu screen. For details, refer to the Cabletron Systems *Port Based VLAN User's Guide*. In this manual, Section 5.15.9 describes how to configure the modules to function as 802.1Q switches.

5.21 SYSTEM RESOURCES SCREEN

The System Resources screen, Figure 5-30, provides information concerning the processor used in the 6H122-16 and the amount of FLASH memory, DRAM, and NVRAM that is installed and how much of this memory is available.

To access the System Resources screen from the Module Specific Configuration menu screen, use the arrow keys to highlight the **SYSTEM RESOURCES** menu item and press ENTER. The System Resources screen displays.

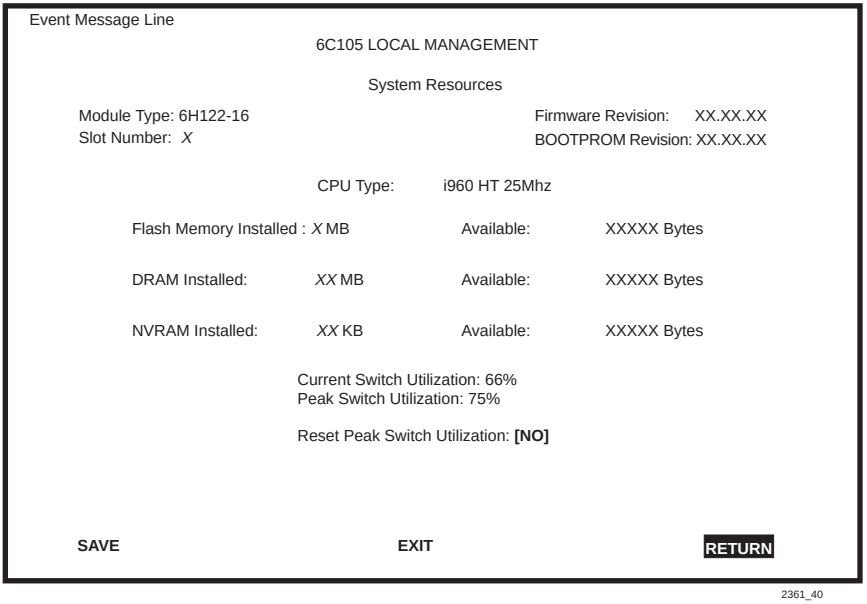


Figure 5-30 System Resources Screen

The following briefly explains each field of the System Resources screen.

CPU Type (Read-only)
Indicates the microprocessor used in the 6H122-16.

Flash Memory Installed (Read-only)
Indicates the amount of FLASH memory installed in the 6H122-16 and how much is currently available.

DRAM Installed (Read-only)
Indicates the amount of DRAM installed in the 6H122-16 and how much of it is currently available.

NVRAM Installed (Read-only)
Indicates the amount of NVRAM installed in the 6H122-16 and how much of it is currently available.

Current Switch Utilization (Read-only)
Shows how much (percentage of capacity) the 6H122-16 is currently being used.

Peak Switch Utilization (Read-only)
Shows the peak percentage of maximum switching capacity, since last reset.

Reset Peak Switch Utilization (Toggle)
Allows the user to reset the Peak Switch Utilization field. The switch may be set to either YES or NO as described in Section 5.21.1. YES resets the Peak Switch Utilization field to the current system traffic.

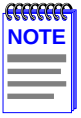
5.21.1 Setting the Reset Peak Utilization

To reset the Reset Peak Utilization field counter, proceed as follows:

1. Use the arrow keys to highlight the **Peak Switch Utilization** field.
2. Press the SPACE bar to select **YES**.
3. Use the arrows keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” is displayed, and the Reset Peak Utilization counter is reset to zero.

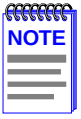
5.22 FLASH DOWNLOAD SCREEN

The Flash Download screen, shown in Figure 5-31, allows the user to clear the information stored in the 6H122-16 FLASH memory and download a new image file from a TFTP server.



The user may also force a download by changing the position of Switch 6 located inside the module. Refer to Section B.2 for details.

Before downloading a new image to the module, load the image onto the network TFTP server.



For information on how to set up a workstation as a TFTP server, refer to the specific workstation documentation.

To access the Flash Download screen from the Module Specific Configuration screen, use the arrow keys to highlight the **FLASH DOWNLOAD** menu item and press ENTER. The Flash Download screen displays.

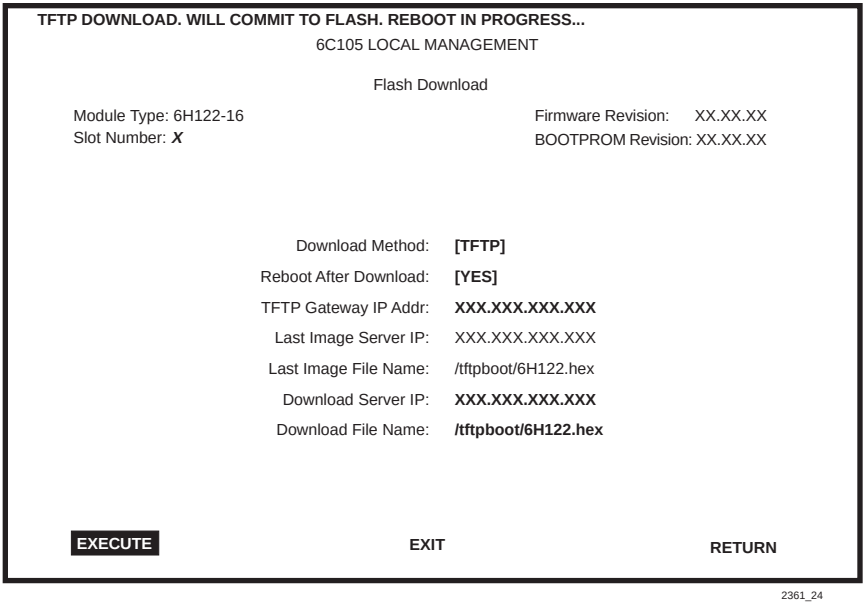
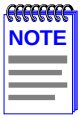


Figure 5-31 Flash Download Screen



Download Server IP and Download Server Filename are displayed only when **TFTP** or **RUNTIME** are selected in Download Method.

The following briefly explains each field of the Flash Download screen:

Download Method (Selectable)
This field steps through TFTP, RUNTIME and BOOTP. If set for BOOTP, the module sends out a BootP request to determine the IP address of the TFTP server and the filename of the image to be downloaded. If set for TFTP or RUNTIME, the 6H122-16 attempts a TFTP download based on the IP address and filename entered in the fields at the bottom of the Flash Download screen. Section 5.22.1 describes how to download using TFTP.

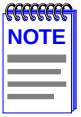
Section 5.22.2 describes how to download using RUNTIME.
Section 5.22.3 describes how to download using BootP.

Reboot After Download (Modifiable when RUNTIME is chosen only)
This field notifies the user that the 6H122-16 will reboot after the download is complete. If a RUNTIME Download is performed, this field toggles between YES and NO. If YES is selected, the module reboots after the download is completed. If NO is selected the module continues using the existing the firmware image. The module stores the new firmware image in FLASH memory. When the module or 6C105 chassis is reset, the module will boot from FLASH memory using the new image.

TFTP Gateway IP Addr (modifiable)
This field shows the IP address of the TFTP gateway server defined in the General Configuration screen in Section 5.15.4.

Last Image Server IP (Read-only)
This field shows the IP address of the server used for the previous FLASH Download.

Last Image File Name (Read-only)
This field shows the complete path and file name of the last image downloaded to FLASH.



If **TFTP** or **RUNTIME** is selected as the download method (Figure 5-31), the following two additional fields appear.

Download Server IP (Selectable)
The IP address of the TFTP server to be used for the FLASH download is entered in this field.

Download File Name (Selectable)
The complete TFTP Server path and file name of the new image is entered in this field.

5.22.1 Image File Download Using TFTP

Set the 6H122-16 to download to FLASH using TFTP as follows:

1. Use the arrow keys to highlight the **Download Method** field.

2. Use the SPACE bar to select **TFTP**.
3. Use the arrow keys to highlight the **TFTP Gateway IP Addr** field.
4. Set the IP address of the TFTP gateway server (this defaults to the same IP address as that set in the TFTP Gateway IP Addr field on the General Configuration screen).
5. Use the arrow keys to highlight the **Download Server IP** field.
6. Enter the IP address of the TFTP server using the DDN format.

   For example: 134.141.79.121
7. Use the arrow keys to highlight the **Download File Name** field.
8. Enter the complete pathway and file name of the image stored on the download server.

   For example: /tftpboot/6H122.hex
9. Use the arrow keys to highlight **EXECUTE** at the bottom of the screen and press ENTER. The message "TFTP DOWNLOAD. WILL COMMIT TO FLASH. REBOOT IN PROGRESS..." displays in the event message line at the top of the screen and the new image is downloaded into FLASH memory.

5.22.2 Image File Download Using RUNTIME

Set the 6H122-16 to download to FLASH using RUNTIME as follows:

1. Use the arrow keys to highlight the **Download Method** field.
2. Use the SPACE bar to select **RUNTIME**.
3. Use the arrow keys to highlight the **Reboot After Download** field.
4. Use the SPACE bar to select either **YES** or **NO**. Select **YES** if you want the module to reboot after the download is completed. Select **NO** if you want the module to store the new image in FLASH memory until the module is manually reset.
5. Use the arrow keys to highlight the **TFTP Gateway IP Addr** field.
6. Set the IP address of the TFTP gateway server (this defaults to the same IP address as that set in the TFTP Gateway IP Addr field on the General Configuration screen).

7. Use the arrow keys to highlight the **Download Server IP** field.
8. Enter the IP address of the TFTP server using the DDN format.

   For example: 134.141.79.121
9. Use the arrow keys to highlight the **Download File Name** field.
10. Enter the complete pathway and file name of the image stored on the download server.

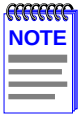
    For example: /tftpboot/6H122.fls
11. Use the arrow keys to highlight **EXECUTE** at the bottom of the screen and press ENTER. The message "RUNTIME DOWNLOAD. WILL COMMIT TO FLASH." displays in the event message line at the top of the screen and the new image is downloaded into FLASH memory.

5.22.3 Image File Download Using BootP

Set the 6H122-16 to download to FLASH using BootP as follows:

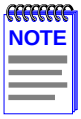
1. Use the arrow keys to highlight the **Download Method** field.
2. Use the SPACE bar to select **BOOTP**.
3. Use the arrow keys to highlight the **TFTP Gateway IP Addr** field. Set the IP address of the TFTP gateway server (this defaults to the same IP address set in the TFTP Gateway IP Addr field in the General Configuration screen).
4. Use the arrow keys to highlight **EXECUTE** at the bottom of the screen and press ENTER. The message "BOOTP DOWNLOAD. WILL COMMIT TO FLASH. REBOOT IN PROGRESS..." displays in the event message line at the top of the screen and the new image is downloaded into FLASH memory.

5.23 PORT REDIRECT FUNCTION SCREEN



The Port Redirect Function screen may not be available depending on the operational mode that has been set for the module. Refer to your Release Notes to see what operational modes support the Port Redirect Function. Refer to Section 5.15.9 for instructions on configuring the operational mode of the module.

The Port Redirect Function screen, Figure 5-32, allows the user to set each one of the ports on the 6H122-16 as a source or destination port. A port can be set to have one or more destination ports. For example, port 1 can be set as a source port with three destinations, ports 2, 3, and 4. Traffic from port 1 is then automatically redirected to ports 2, 3, and 4. Port 1 can also serve as a destination port for other ports. The port redirect function is extremely useful for troubleshooting purposes, as it allows traffic to be sent to a particular port(s) where, with the use of an analyzer or RMON probe, all current traffic from the source port(s) can be examined.



Although all traffic from the source port (including, if desired, errored frames) is sent to the destination port, normal switching is still performed for all frames on the source port.

To access the Port Redirect Function screen from the Module Specific Configuration screen, use the arrow keys to highlight the **PORT REDIRECT FUNCTION** menu item and press ENTER. The Port Redirect Function screen displays.

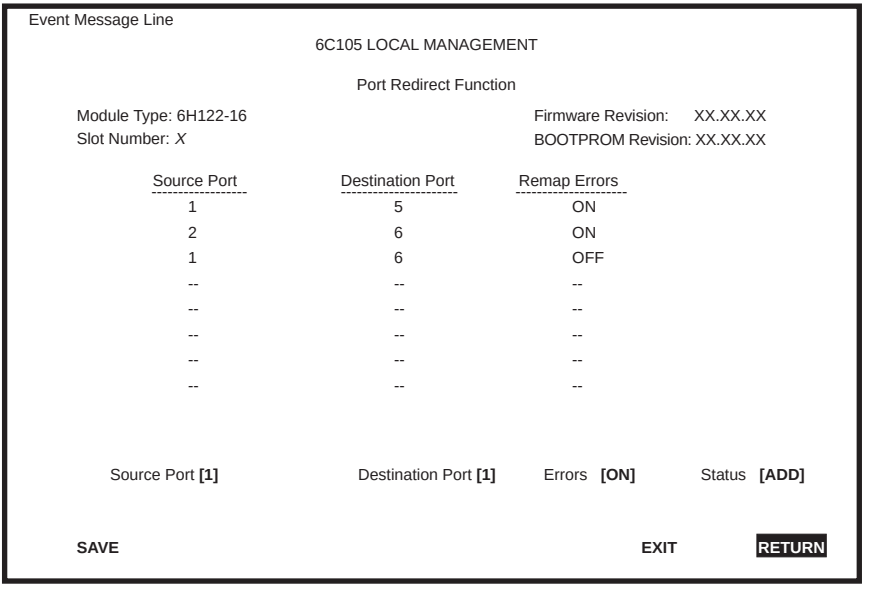


Figure 5-32 Port Redirect Function Screen

The following definitions briefly explain each field of the Port Redirect Function screen:

Source Port (Read-only)
Shows which ports are currently set as source ports.

Destination Port (Read-only)
Shows which ports are currently set as destination ports.

Remap Errors (Read-only)
Displays whether the corresponding source ports are configured to send errored frames to the destination ports (ON), or to drop all errored frames before forwarding traffic (OFF).

Source Port [*n*] (Selectable)
Allows a selected port [*n*] to be changed to a source port.

Destination Port [*n*] (Selectable)
Allows a selected port [*n*] to be changed to a destination port.

Errors (Toggle)
Allows the user to configure the source ports to either send errored frames to selected destination ports (ON option), or to drop errored frames, and send only valid traffic to the destination ports (OFF option). The default setting of this field is ON.

Status (Toggle)
Allows you to add or delete the source and destination ports selected in the Source Port [n] and Destination Port [n] fields.

NEXT/PREVIOUS (Navigation Field)
There can be more than one Port Redirect Function screen depending on the number of port redirect entries. To get to the second or subsequent screens, there is a NEXT field at the bottom of the screen that the user can arrow key over to and highlight. Pressing the ENTER key displays the next screen. In the new screen, the navigation field PREVIOUS will display to allow the user to go back to the first or previous screens.

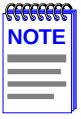
5.23.1 Changing Source and Destination Ports

Add or delete source port and destination port entries as follows:

1. Use the arrow keys to highlight the **Source Port** field.
2. Press the SPACE bar or BACKSPACE one or more times to increment or decrement the port number displayed in the brackets [*n*] until the appropriate port number is displayed.
3. Use the arrow keys to highlight the **Destination Port** field.
4. Use the SPACE bar or BACKSPACE to step to the appropriate port number for the destination port.
5. Use the arrow keys to highlight the **Errors** field.
6. Use the SPACE bar to select either the **ON** or **OFF** option and press ENTER. **ON** forces the source module and port to forward errored frames to the destination module(s) and port(s). **OFF** forces the errored frames to be dropped before forwarding traffic.

7. Use the arrow keys to highlight the **Status** field.

8. Use the SPACE bar to select either the **ADD** or **DEL** (delete) option. Press ENTER. This adds or deletes the port selections made in steps 2 and 4 and also updates the screen Source Port and Destination Port list.

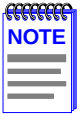


If more than one port is to be redirected, repeat steps 1 through 8 for each additional setting, then go to step 9 to save all the new settings at once.

9. Use the arrow keys to highlight **SAVE** at the bottom of the screen. Press ENTER. The message "SAVED OK" is displayed.

5.24 BROADCAST SUPPRESSION SCREEN

The Broadcast Suppression screen, Figure 5-33, allows the user to set a desired limit of receive broadcast frames that are switched out to the other ports.



The Broadcast Suppression screen may not be available if the operational mode of the module has been set to SECURE FAST VLAN. Refer to your Release Notes to see what operational modes support Broadcast Suppression. Refer to Section 5.15.9 for instructions on configuring the operational mode of the module.

Any broadcast frames received above the desired threshold will be dropped.

To access the Broadcast Suppression screen from the Module Specific Configuration screen, use the arrow keys to highlight the **BROADCAST SUPPRESSION** menu item and press ENTER. The Broadcast Suppression screen displays.

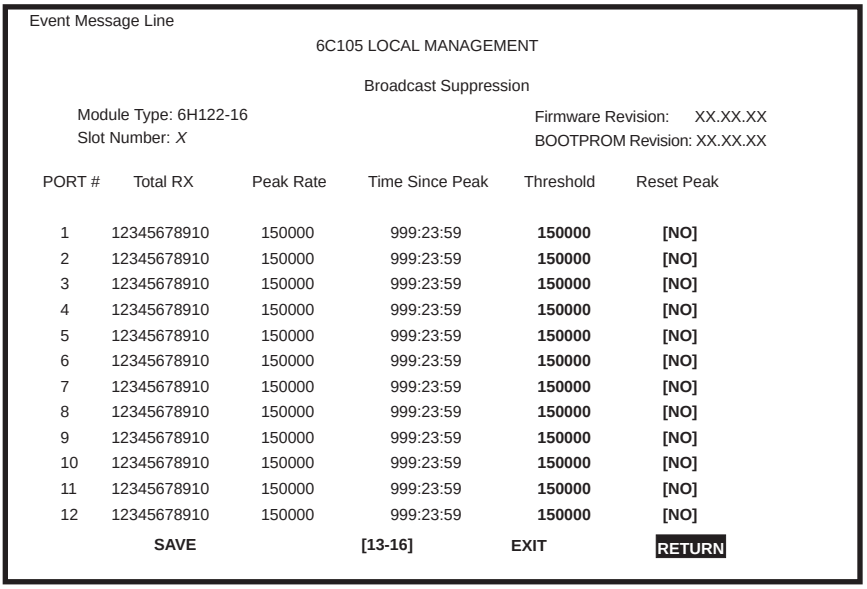


Figure 5-33 Broadcast Suppression Screen

The following explains each field of the Broadcast Statistics screen:

PORT # (Read-only)
Identifies the number of the port.

Total RX (Read-Only)
Displays the total number of broadcast frames received.

Peak Rate (Read-Only)
Displays the number of broadcast frames received per second.

Time Since Peak (Read-Only)
Displays the time since peak broadcast frames received.

Threshold (Modifiable)
Allows the user to set the desired limit of receive broadcast frames that will be forwarded per port per second.

Reset Peak (Toggle)
Allows the user to reset the peak rate. Resetting the Peak Rate also resets the Time Since Peak field. The Reset Peak field toggles between YES and NO.

[1-12], or [13-16] (Navigation Field)
When the Broadcast Statistics screen displays, the current statistics are displayed for the first 12 ports. This field allows the user to step to a second screen for the same type of information for ports 13 through 16. While on the second screen, the user can navigate back to the first screen by selecting the **[1-12]** field. This is accomplished by using the arrow keys to highlight the field, and then pressing ENTER. The user can change the Threshold or Reset Peak Rate fields while in the first or second screens.

5.24.1 Setting the Threshold

To set the Threshold, proceed as follows:

1. Use the arrow keys to highlight the **Threshold** field for the selected port.
2. Type in the numbers for the desired limit in increments of 10.
3. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen.
4. Press ENTER. The message “SAVED OK” is displayed.

5.24.2 Setting the Reset Peak Switch

To reset the Reset Peak Switch counter to zero, proceed as follows:

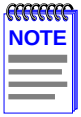
1. Use the arrow keys to highlight the **Reset Peak** field for the selected port.
2. Press the SPACE bar to select **YES**.

3. Use the arrows keys to highlight the **SAVE** command at the bottom of the screen.

4. Press ENTER. The message “SAVED OK” is displayed, and the Reset Peak Switch counter is reset to zero.

5.25 MODULE STATISTICS MENU SCREEN

The Module Statistics Menu screen, Figure 5-34, provides access to screens that allow the user to obtain switch statistics about frame traffic through each interface, to view MIB-II statistics from each interface, and to view RMON Statistics gathered by the RMON agent embedded in the 6H122-16.



The SWITCH STATISTICS menu item on the Module Statistics Menu screen will not display if the operational mode of the module has been set to SECURE FAST VLAN.

Section 5.15.9 provides instructions on setting the operational mode.

To access the Module Statistics Menu from the Module Menu screen, use the arrow keys to highlight the **MODULE STATISTICS** menu item and press ENTER. The Module Statistics Menu screen displays.

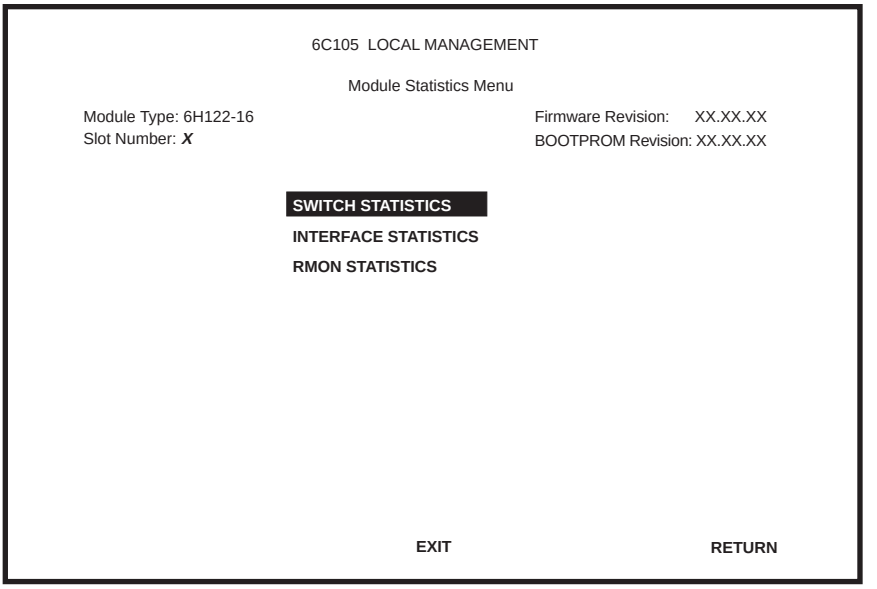


Figure 5-34 Module Statistics Menu Screen

The Module Statistics Menu screen displays the following menu items:

SWITCH STATISTICS

The Switch Statistics screen lists the number of frames received, transmitted, filtered, and forwarded by each interface.

INTERFACE STATISTICS

The Interface Statistics screen provides the MIB-II statistics for each switched interface, on an interface-by-interface basis.

RMON STATISTICS

The RMON Statistics screen displays all the statistics gathered by the embedded RMON agent built-in to the 6H122-16.

5.26 SWITCH STATISTICS SCREEN

The Switch Statistics screen, Figure 5-35, lists the number of frames received, transmitted, filtered, and forwarded by each interface, including backplane interfaces.

NOTES

The Switch Statistics screen will not be available if the operational mode of the module has been set to SECURE FAST VLAN. This screen may only be used by modules configured to operate as 802.1D or 802.1Q switches.

Ports 17 through 20 represent the backplane connections that the 6H122-16 has with the 6C105 chassis. The module has a direct connection to every other slot in the chassis.

To access the Switch Statistics screen from the Module Statistics Menu screen, use the arrow keys to highlight the **SWITCH STATISTICS** menu item and press ENTER. The Switch Statistics screen displays.

Event Message Line

6C105 LOCAL MANAGEMENT

Switch Statistics

Module Type: 6H122-16
Slot Number: ***X***

Firmware Revision: XX.XX.XX
BOOTPROM Revision: XX.XX.XX

Port #	Frames Rcvd	Frames Txmtd	Frames Fltrd	Frames Frwded
1	100	100	0	100
2	100	100	0	100
3	100	100	0	100
4	100	100	0	100
5	100	100	0	100
6	100	100	0	100
7	100	100	0	100
8	100	100	0	100
9	100	100	0	100
10	100	100	0	100
11	100	100	0	100
12	100	100	0	100
13	100	100	0	100

CLEAR COUNTERS **NEXT** **EXIT** **RETURN**

2361_28

Figure 5-35 Switch Statistics Screen

The Switch Statistics screen displays the following items:

Port # (Read-Only)
Identifies the interface or port number.

Frames Rcvd (Read-Only)
Displays the number of frames received by the interface.

Frames Txmtd (Read-Only)
Displays the number of frames transmitted by the interface.

Frames Fltrd (Read-Only)
Displays the number of frames filtered by the interface.

Frames Frwded (Read-Only)
Displays the number of frames forwarded by the interface.

CLEAR COUNTERS (Command)
This command is used to reset all statistic counters to zero. For details on how to use this field, refer to Section 5.26.1.

NEXT/PREVIOUS (Navigation Field)
The first time the Switch Statistics screen comes up, there is a NEXT field that the user can arrow key over and highlight. Pressing the ENTER key displays the next screen. In the new screen, the navigation field PREVIOUS will display to allow the user to go back to the first screen.

5.26.1 Using the Clear Counters Command

To reset all the statistics counters to zero, perform the following steps:

1. Use the arrow keys to highlight the **CLEAR COUNTERS** field.
2. Press ENTER, the counters for the selected port are reset to zero.

5.27 INTERFACE STATISTICS SCREEN

The Interface Statistics screen is used to gather MIB-II statistics for all of the 6H122-16 interfaces (ports 1 through 16 and all backplane interfaces).

To access the Interface Statistics screen, use the arrow keys to highlight the **INTERFACE STATISTICS** menu item on the Module Statistics Menu screen and press ENTER. The Interface Statistics screen, Figure 5-36, displays.

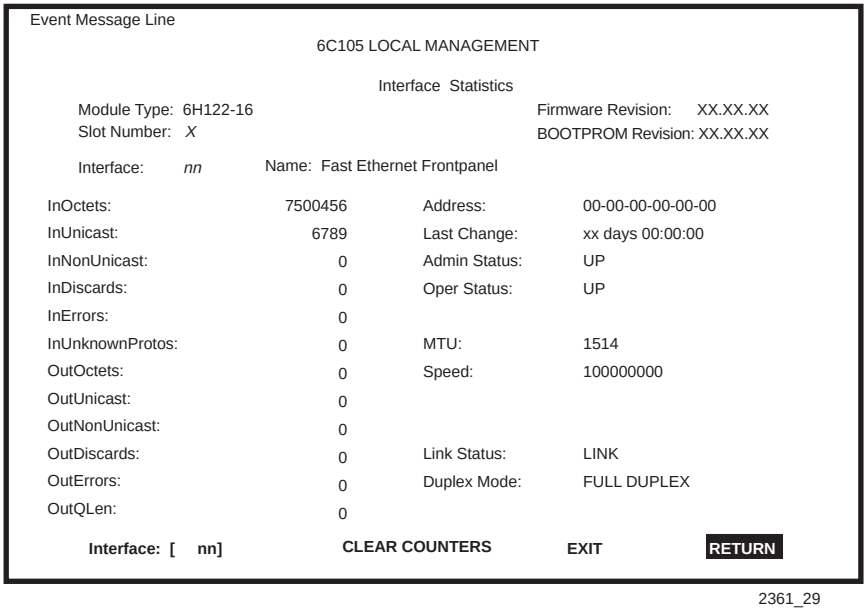


Figure 5-36 Interface Statistics Screen

The following definitions explain each field of the Interface Statistics screen:

Interface (Read-only)

This field displays the Interface number for which statistics are currently being displayed. Figure 5-36 shows the Interface field displaying 1. This represents interface 1 of the module. To view other interface statistics, refer to Section 5.27.1.

Name (Read-only)
The Name field displays the type of interface for which statistics are being displayed.

InOctets (Read-only)
This field displays the total number of octets (bytes) that have been received on the interface. This includes all octets from bad frames, and framing characters.

InUnicast (Read-only)
The InUnicast field displays the total number of frames that have been received that were sent to a single address.

InNonUnicast (Read-only)
This field displays the total number of frames that have been received that were delivered to a broadcast or multicast address.

InDiscards (Read-only)
The InDiscards field displays the total number of inbound frames that were discarded, even though the frames contained no errors. This field may increment because the switch needed to free up buffer space, or the switch was being overutilized.

InErrors (Read-only)
This field displays the total number of inbound frames that have been discarded because they contained errors. This field represents the total number of errored frames, regardless of the cause of the error.

InUnknownProtos (Read-only)
The InUnknownProtos field displays the total number of frames that were discarded because the frames were in an unknown, or unsupported, format.

OutOctets (Read-only)
This field displays the total number of octets (bytes) that have been transmitted from the interface.

OutUnicast (Read-only)
The OutUnicast field displays the total number of frames transmitted that were sent to a single address.

OutNonUnicast (Read-only)
This field displays the total number of frames transmitted to a broadcast or multicast address.

OutDiscards (Read-only)
The OutDiscards field displays the total number of outbound frames that were discarded, even though the frames contained no errors. This field may increment because the switch needed to free up buffer space, or because the switch was being overutilized.

OutErrors (Read-only)
This field displays the total number of outbound frames discarded because they contained errors. This field represents the total number of errored frames, regardless of the cause of the error.

OutQLen (Read-only)
The OutQLen field displays the length of the frame queue. The field represents the total number of frames that can be contained in the queue.

Address (Read-only)
This field displays the MAC Address of the interface that is currently being displayed.

Last Change (Read-only)
This field displays the last time that the interface was reset.

Admin Status (Read-only)
This field displays the current status of the interface. If this field displays “Testing”, no frames may be passed on this interface.

Oper Status (Read-only)
This field displays the current status of the interface. If this field displays “Testing”, no frames may be passed on this interface.

MTU (Read-only)
The MTU field displays the maximum frame size (in octets) that a frame may contain to be received or transmitted from this interface.

Speed (Read-only)
The Speed field displays the theoretical maximum amount of bandwidth that the interface can support in bits per second.

Link Status (Read-only)
This field displays the current link status of the interface. This field will read either “LINK” or “NO LINK”.

Duplex Mode (Read-only)
This field indicates whether the interface is operating in normal or full duplex mode. This field will read either “STANDARD” or “FULL DUPLEX”.

Interface [nn] (Command)
This command is used to enter an interface number for viewing statistics. For instructions on how to use this command, refer to Section 5.27.1.

CLEAR COUNTERS (Command)
This command is used to reset all statistic counters to zero. For details on how to use this field, refer to Section 5.27.2.

5.27.1 Displaying Interface Statistics

To display the statistics for any interface, proceed as follows:

1. Use the arrow keys to highlight the **Interface [nn]** field at the bottom of the screen.
2. Press the SPACE bar to increment (or press the DEL [delete] key to decrement) the interface number.
3. Press ENTER (neither the **Interface #** fields nor the statistics will change until ENTER is pressed).

5.27.2 Using the Clear Counters Command

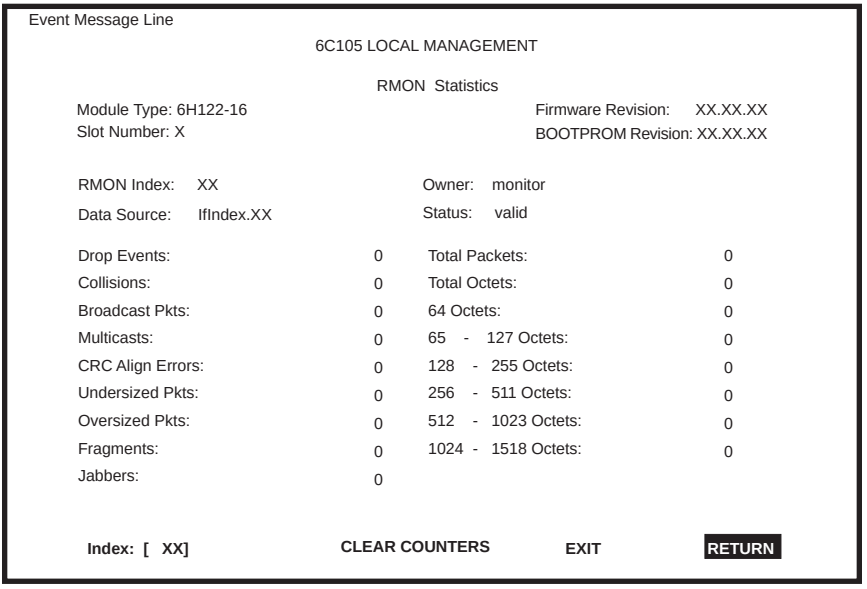
To reset all the statistics counters of the selected interface to zero, perform the following steps:

1. Use the arrow keys to highlight the **CLEAR COUNTERS** command.
2. Press ENTER, the counters for the selected interface are reset to zero.

5.28 RMON STATISTICS SCREEN

RMON statistics for each interface, on a interface-by-interface basis, are viewed through the RMON Statistics screen shown in Figure 5-37.

To access the RMON Statistics screen, use the arrow keys to highlight the **RMON STATISTICS** menu item on the Module Statistics Menu screen and press ENTER. The RMON Statistics screen displays.



2361_65

Figure 5-37 RMON Statistics Screen

The following definitions explain each field of the RMON Statistics screen:

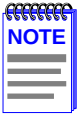
RMON Index (Read-only)
This field displays the current Ethernet interface for which statistics are being shown. The 6H122-16 has an embedded RMON agent that gathers statistics for each interface on the module.

Data Source (Read-only)
This field displays the source of the statistics data that is currently being displayed on the screen. Figure 5-37 shows that the data source for this RMON index is Interface XX by displaying the name IfIndex.XX. If the screen was displaying RMON statistics for Interface 1 (port 1), the name displayed would be IfIndex.1.

Owner (Read-only)
This field displays the name of the entity that configured this entry.

Status (Read-only)
The Status field displays the current operating status of the displayed interface. This field will display “valid” or “invalid”.

Drop Events (Read-only)
This field displays the total number of times that the RMON agent was forced to discard frames due to the lack of available switch resources.



The Drop Events field does not display the actual number of frames dropped, it only displays the number of times that the RMON agent was forced to discard frames.

Collisions (Read-only)
This field displays the total number of collisions that have occurred on this interface.

Broadcast Pkts (Read-only)
The Broadcast Pkts field displays the total number of good frames that were directed to the broadcast address. The value of this field does not include multicast frames.

Multicasts (Read-only)
The Multicasts field displays the total number of good frames received that were directed to a multicast address. The value of this field does not include frames directed to the broadcast address.

CRC Align Errors (Read-only)
This field displays the number of frames with bad Cyclic Redundancy Checks (CRC) or misaligned frames received from the network. The CRC is a 4-byte field in the data frames that ensures that the data received is the same as the data that was originally sent.

Undersized Pkts (Read-only)
The Undersized Pkts field displays the number of frames received whose size was less than the minimum Ethernet frame size of 64 bytes, not including preamble, but have a valid CRC.

Oversized Pkts (Read-only)
The Oversized Pkts field displays the number of frames received whose size exceeded 1518 data bytes, not including preamble, but have a valid CRC.

Fragments (Read-only)
The total number of undersized frames with a bad CRC.

It is normal for the Fragments field to increment. This is because the RMON agent increments the field when undersized frames (frames less than 64 bytes) are detected, which are normal occurrences due to collisions, and when noise hits occur.

Jabbers (Read-only)
This field displays the total number of frames that were greater than 1518 bytes and had a bad CRC.

Total Packets (Read-only)
This field displays the total number of frames (including bad frames, broadcast frames, and multicast frames) received on this interface.

Total Octets (Read-only)
This field displays the total number of octets (bytes) of data, including those in bad frames, received on this interface.

64 Octets (Read-only)
Displays the total number of frames including bad frames, received that were 64 bytes in length (excluding framing bits, but including CRC bytes).

65 - 127 Octets (Read-only)
Displays the total number of frames, including bad frames, received that were between 65 and 127 bytes in length (excluding framing bits, but including CRC bytes).

128 - 255 Octets (Read-only)
Displays the total number of frames, including bad frames, received that were between 128 and 255 bytes in length (excluding framing bits, but including CRC bytes).

256 - 511 Octets (Read-only)
Displays the total number of frames, including bad frames, received that were between 256 and 511 bytes in length (excluding framing bits, but including CRC bytes).

512 - 1023 Octets (Read-only)
Displays the total number of frames, including bad frames, received that were between 512 and 1023 bytes in length (excluding framing bits, but including CRC bytes).

1024 - 1518 Octets (Read-only)
Displays the total number of frames, including bad frames, received that were between 1024 and 1518 bytes in length (excluding framing bits, but including CRC bytes).

Index [nn] (Command)
This command is used to enter an index number for viewing statistics. For instructions on how to use this command, refer to Section 5.28.1.

CLEAR COUNTERS (Command)
This command is used to reset all statistic counters to zero. For details on how to use this field, refer to Section 5.28.2.

5.28.1 Displaying RMON Statistics

To display the statistics for any index, proceed as follows:

1. Use the arrow keys to highlight the **Index [nn]** field at the bottom of the screen.
2. Press the SPACE bar to increment (or press the DEL [delete] key to decrement) the index number.
3. Press ENTER (neither the **RMON Index** field nor the statistics will change until ENTER is pressed).

5.28.2 Using the Clear Counters Command

To reset all the statistics counters of the selected interface to zero, perform the following steps:

1. Use the arrow keys to highlight the **CLEAR COUNTERS** field.
2. Press ENTER, the counters for the selected index are reset to zero.

5.29 NETWORK TOOLS

The Network Tools function resides on the 6H122-16 and allows the user to access and manage network devices.

To access the Network Tools screen, use the arrow keys to highlight the **NETWORK TOOLS** menu item in the Module Menu screen and press ENTER. The Network Tools screen displays.

Type **help** at the prompt to list all the commands that are available for the module in the current operational mode. See Figure 5-38. A command used incorrectly (wrong syntax), will prompt a display of the correct usage.

Use lower case when entering commands in Network Tools.

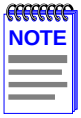
```
Welcome to Network Tools

-> help

  Commands Available to the User:

    Built in Commands:

     arp              bridge           defroute
    netstat           ping             reset
    show              traceroute

    soft_reset       telnet            link_trap


    SPECIAL:
        done, quit, or exit - Exit from the Network Tools.
        For help with a specific command, type 'help <command>'.
->
```

Figure 5-38 Network Tools Help Screen

The Network Tools functions are performed using a series of commands. Entering commands in Network Tools involves typing the command to be executed at the Network Tools prompt, adding any desired or required extensions, and pressing ENTER.

There are two categories of commands in the command set.

- Built-in Commands – Allow the user to access and manage network devices. The commands are **arp**, **bridge**, **defroute**, **netstat**, **ping**, **reset**, **show**, **traceroute**, **soft_reset**, **telnet**, and **link_trap**.
- Special Commands – Allow the user to exit from Network Tools. The commands are **done**, **exit**, and **quit**.



The conventions used in describing the commands in Network Tools are as follows:

Arguments enclosed by [ ] are required.

Arguments enclosed by < > are optional.

In the following command examples, the information entered by the user is shown in **bold** Helvetica font.

To abort the output or interrupt a process, press the CONTROL key and c key simultaneously, designated as ^C here.

The commands are presented in the following format:

command:

Syntax:	Shows the required command format. It indicates where arguments, if any, must be specified.
Description:	Briefly describes the command and its uses.
Options:	Lists any additional fields in the appropriate format that may be added to the command.
Example:	Shows an example of the command.

5.29.1 Built-in Commands

The built-in commands listed in this section activate functions on the managed device or devices being accessed through Network Tools.

arp:

Syntax: arp [options]

Description: The arp command provides access to the ARP (Address Resolution Protocol) cache, enabling you to view cache data, delete entries, or add a static route. Super-User access is required to delete an entry or add a static route.

Each ARP cache entry lists the network *interface* that the device is connected to, the device's *network address* or IP address, the device's *physical address* or MAC address, and the *media type* of connection to the device. Media types are displayed as numbers, which stand for the following states:

1 - Other
2 - Invalid entry (cannot ping device, timed out, etc.)
3 - Dynamic route entry
4 - Static route entry (not subject to change)

You can specify the arp command without options, or with one of the following options:

Options:
-a Views cache data
-d Deletes an IP address entry. Requires additional arguments: [Interface Number] [IP address]
-s Adds a static entry. Requires additional arguments: [Interface Number] [IP address] [MAC address]
-f Flushes the ARP cache

Example:

```
-> arp -a
# Interface          Network Address     Physical Address    Media Type
# (SonicInt)         122.144.40.111      00.00.0e.12.3c.04   3(dynamic)
# (SonicInt)         122.144.48.109      00.00.0e.f3.3d.14   3(dynamic)
# (SonicInt)         122.144.52.68       00.00.0e.12.3c.04   3(dynamic)
# (SonicInt)         122.144.21.43       00.00.0e.03.1d.3c   3(dynamic)


-> arp -d 1 122.144.52.68


-> arp -s 1 22.44.2.3 00:00:0e:03:1d:3c


-> arp -f
```

051467

bridge:

Syntax: bridge [ENABLE/DISABLE] [IFNUM/ALL]

Description: The bridge command allows each bridge port to be enabled or disabled at the user's request, either one at a time or all at once. Specifying a single interface number will affect the bridging status of that interface, while specifying ALL will affect every interface.

Options: Not Applicable

Example:

```
-> bridge disable all


-> bridge enable 1


-> bridge disable 1
```

051468

defroute:

Syntax: defroute [interface number] [IP address]
defroute <delete>

Description: The defroute command allows the user to view, set or delete the default IP route to a managed device through the specified interface.

Options: Not Applicable

Example:

```
-> defroute 2 147.152.42.32
   # Default route is 147.152.42.32 on interface 2
-> defroute
   # Default route is 147.152.42.32 on interface 2
-> defroute delete
   # Default route is not currently set.
->
```

05141-69

netstat:

Syntax: netstat [option]

Description: The netstat command provides a display of general network statistics for the managed device. The netstat command must be used with one of the two display options.

Options: -i Displays status and capability information for each interface
-r Displays routing information for each interface

Example:

```
-> netstat -i
Interface + Description     MTU     Speed      Admin   Oper   MAC Addr

# 1 (ethernet -csmacd)      1514    10000000   up      up     0x00 0x00 0x1d 0x07 0x50 0x0e
# 2 (ethernet - csmacd)     1514    10000000   up      up     0x00 0x00 0x1d 0x07 0x50 0x0f
# 3 (ethernet - csmacd)     1514    10000000   up      up     0x00 0x00 0x1d 0x07 0x50 0x10
# 4 (ethernet - csmacd)     1514    10000000   up      up     0x00 0x00 0x1d 0x07 0x50 0x11

-> netstat -r
Destination                 Next-hop                Interface

# Default Route             DirectConnection        1
# 134.141.0.0               DirectConnection        2
# 134.141.0.0               DirectConnection        3
```

051470

ping:

Syntax: ping [IP address]

Description: The ping command generates an outbound ping request to check the status (alive/not alive) of a device at a specified IP address.

Options: Not Applicable

Example:

```
-> ping 122.144.40.10
122.144.40.10 is alive
```

051471

reset:

Syntax: reset

Description: The reset command allows a soft reset of the device. The user will be queried to confirm the reset command to insure against unwanted resets.

The Network Tools connection to the module will be terminated upon execution of this command.

Options: Not Applicable

Example:

```
-> reset
RESET:Are you *SURE*? ->Y
```

174245

show:

Syntax: show [PROTOCOL] <TABLE>

Description: The show command displays information concerning various components of the device. Protocols currently supported are IP, IPX, DECnet, and AppleTalk. Components of those protocols that are currently supported are ARP caches, route tables, FIB tables, server tables, and interface tables. The number of valid entries in the table will be displayed at the end of the table display.

Options: Not Applicable

Example:

```
-> show Appletalk interfaces

# Interface   AdminStatus   OperStatus   MTU    Forwarding   Framing
# 1           enabled       enabled      1500   enabled      ethernet
# 2           disabled      disabled     1500   disabled     ethernet


-> show IP ARP

# Interface   MediaType     PhysicalAddress     NetworkAddress
# 3           3 (dynamic)   00:00:1d:04:40:5d   123.456.40.1
# 4           3 (dynamic)   08:00:20:0e:d8:31   123.456.40.30
```

174246

traceroute:

Syntax: traceroute [IP address]

Description: The traceroute command generates a TRACEROUTE request to a specified IP address and provides a display of all next-hop routers in the path to the device. If the device is not reached, the command displays all next-hop routers to the point of failure.

Options: Not Applicable

Example:

```
-> traceroute 122.144.11.52

# next-hop[0] : 122.144.60.45
# next-hop[1] : 122.144.8.113
# next-hop[2] : 122.144.61.45
# 122.144.11.52 is alive : 3 hops away.
```

051477

soft_reset:

Syntax: soft_reset

Description: This command restarts the software image, which restores the user configuration settings from NVRAM. The user will be queried to confirm the reset command to ensure against unwanted resets.

The Network Tools connection to the module will be terminated upon execution of this command.

Options: Not Applicable

Example:

```
-> soft_reset
RESET: Are you *SURE*? -> Y
```

174266

telnet:

Syntax: telnet [IP address] <Port #>

Description: The telnet command allows the user to communicate with another host (that supports Telnet connections) using the Telnet protocol. The user must specify the remote host using its IP address. The [IP address] field is mandatory. If no Port number is specified, telnet will attempt to contact the host at the default port.

Options: Not Applicable

Example:

```
-> telnet 134.141.12.345
Trying 134.141.12.345
Connected to 134.141.12.345

SunOS UNIX (server1)

login:
```

link_trap:

Syntax: link_trap [enable/disable/status] <PORT/all>

Description: The link_trap command allows link traps to be enabled or disabled when specifying a single port, or simultaneously when specifying “all” or no ports. When one or all ports are specified to enable, disable, or find their status, their current condition is displayed.

Options: Not Applicable

Example:

```
-> link_trap status
LINK TRAP STATUS:

  Port 1  is ENABLED          Port 2  is DISABLED
  Port 3  is ENABLED          Port 4  is ENABLED

-> link_trap disable 2
Link traps have been DISABLED on port 2

-> link_trap disable all
Link traps have been DISABLED on all ports (1-16)

-> link_trap status 3
Link traps are ENABLED on port 3
```

5.29.2 Special Commands

done, quit, exit:

Syntax: done

Description: The done command enables the user to exit from Network Tools and return to the Main Menu screen.

Options: Not Applicable

Example:

```
-> done
```

APPENDIX A

SPECIFICATIONS

This appendix provides operating specifications for the Cabletron Systems 6H122-16 Interface Modules. Cabletron Systems reserves the right to change these specifications at any time without notice.

A.1 DEVICE SPECIFICATIONS

Processor:	Intel i960 RISC processor control
Dynamic Random Access Memory (DRAM):	16 MB
FLASH Memory:	4 MB

A.2 PHYSICAL PROPERTIES

Dimensions:	43.87 H x 5.71 W x 27.88 D (cm) 18.28 H x 2.38 W x 11.62 D (in)
Weight (Unit):	2.72 kg (6 lb)
MTBF (Predicted):	200,000 hours

A.3 ENVIRONMENTAL REQUIREMENTS

Operating Temperature:	5°C to 40°C (41°F to 104°F)
Storage Temperature:	-30°C to 73°C (-22°F to 164°F)
Operating Relative Humidity:	5% to 90% (non-condensing)

A.4 INPUT/OUTPUT PORTS

6H122-16 Specifications

Ports 1 through 16	Fast Ethernet 10/100 Mbps (100BASE-TX compliant) with RJ45 type connectors.

A.5 COM PORT PINOUT ASSIGNMENTS

The COM port is a serial communications port that supports Local Management or connection to a UPS.

The COM port has the following pin assignments:

Table A-1 COM Port Pin Assignments

Pin	Signal Name	Input/Output
1	Transmit Data (XMT)	Output
2	Data Carrier Detect (DCD)	Output
3	Data Set Ready (DSR)	Input
4	Receive Data (RCV)	Input
5	Signal Ground (GND)	NA
6	Data Terminal Ready (DTR)	Output
7	Request to Send (RTS)	Input
8	Clear to Send (CTS)	NA

A.6 REGULATORY COMPLIANCE

Safety

The 6H122-16 meets the safety requirements of UL 1950, CSA C22.2 No. 950 and EN 60950, IEC 950, and 73/23/EEC.

Electromagnetic Compatibility (EMC)

The 6H122-16 meets the requirements of FCC Part 15, EN 50082-1, EN 55022, VCCI V-3, CSA C108.8, AS/NZS 3548 and 89/336/EEC.

APPENDIX B
MODE SWITCH BANK SETTINGS

This appendix covers the following items:

- Required tools (Section B.1)
- Locations, functions, and settings for the mode switches (Section B.2)

B.1 REQUIRED TOOLS

You need the following tools to perform the procedures provided in this appendix:

- Antistatic wrist strap (provided with 6C105 chassis)

B.2 SETTING THE MODE SWITCH

These switches are set at the factory and do not need to be changed unless you intend to perform the following:

- Force download a new image file from a BootP server.
- Clear NVRAM and restore all user-entered parameters such as the IP address and Subnet Masks to the 6H122-16 “Default” configuration settings.
- Clear user-entered passwords stored in NVRAM and restore the default passwords.

The 6H122-16 is sensitive to static discharges. Use an antistatic wrist strap and observe all static precautions during this procedure. Failure to do so could damage the 6H122-16.

Figure B-1 shows the location of the mode switches and the switch settings for normal operation.

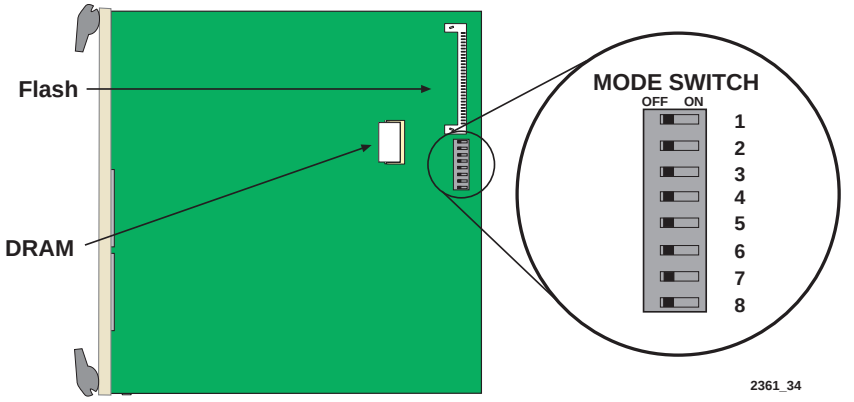


Figure B-1 6H122-16 Mode Switch Location/Component Layout

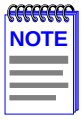
Switch definitions and positions are as follows:

- Switches 1 through 4 – For Cabletron Systems use only.
- Switch 5 – COM Port Autobaud. The default (OFF) position enables Autobaud sensing on the COM port for Local Management sessions. Changing the switch to the ON position disables Autobaud sensing and sets the COM port to 9600 baud for Local Management sessions.
- Switch 6 – Forced BootP. Changing the position of this switch (i.e., moving the switch from one position to the other) clears download information from NVRAM and forces the 6H122-16 to download a new image file from a BootP server after power to the chassis is restored.

NOTE

After changing the position of switch 6, DO NOT reapply power to the chassis until there is a station acting as a BootP server, which contains the image file.

- After changing the position of switch 6 and restarting the module, the 6H122-16 requests a new image download until they either receive a new image or the RESET button on the front panel is pressed. When the RESET button is pressed, the 6H122-16 continues trying to contact a BootP server, but will time out in approximately one minute. If the module times out, the image is downloaded from its FLASH memory.
- Switch 7 – Clear NVRAM. Changing the position of this switch resets NVRAM on the next power up. ALL user entered parameters, such as IP addresses, subnet masks, SNMP traps, and switching functions are restored to their factory default settings.
- Switch 8 – Reset Password/Community Strings. Changing the position of this switch clears only the user-entered passwords stored in NVRAM, and restores the default passwords. Once the 6H122-16 resets, the passwords can either be reentered or the default passwords (Public and ENTER) may be used.



Do not change the position of switch 8 unless it is necessary to reset the module super-user configured passwords to their factory default settings.

INDEX

T

U