System Release 7.17
ASTRO® 25
INTEGRATED VOICE AND DATA

MAC Port Lockdown

NOVEMBER 2016

MN003324A01-A

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

Furthermore, the purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a particular system, or may be dependent upon the characteristics of a particular mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

This page intentionally left blank.

Contact Us

Motorola Solutions Support Center

The Solutions Support Center (SSC) is the primary Motorola Solutions support contact. Call:

- Before any software reload.
- To confirm troubleshooting results and analysis before removing and replacing a Field Replaceable Unit (FRU) and Field Replaceable Entity (FRE) to repair the system.

For...	Phone
United States Calls	**800-221-7144**
International Calls	**302-444-9800**

North America Parts Organization

For assistance in ordering replacement parts or identifying a part number, contact the Motorola Solutions Parts organization. Your first response when troubleshooting your system is to call the Motorola SSC.

For...	Phone
Phone Orders	**800-422-4210** (US and Canada Orders) For help identifying an item or part number, select choice 3 from the menu.
	302-444-9842 (International Orders) Includes help for identifying an item or part number and for translation as needed.
Fax Orders	**800-622-6210** (US and Canada Orders)

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number with the error
- A description of the error

We welcome your feedback on this and other Motorola Solutions manuals. To take a short, confidential survey on Motorola Solutions Customer Documentation, go to docsurvey.motorolasolutions.com or scan the following QR code with your mobile device to access the survey.

This page intentionally left blank.

Document History

Version	Description	Date
MN003324A01-A	Original release of the *MAC Port Lockdown* manual.	November 2016

This page intentionally left blank.

Contents

Copyrights **3**
Contact Us **5**
Document History **7**
List of Figures **13**
List of Tables **15**
List of Processes **17**
List of Procedures **19**
About MAC Port Lockdown **21**
What is Covered In This Manual? 21
Helpful Background Information 21
Related Information 21
Chapter 1: MAC Port Lockdown Description **23**
1.1 Ethernet Port Security 23
1.2 MAC Port Lockdown 23
1.3 Ethernet Port Security in ASTRO 25 Systems 24
1.3.1 Switches Supporting Ethernet Port Security in ASTRO 25 System 25
1.4 Location of Ports on the GCP 8000 Site Controller 26
1.5 Location of Ports on the GPB 8000 Reference Distribution Module 27
1.6 Location of Ports on HP Switches 27
1.7 Additional Security with Fiber Optic Ports 29
Chapter 2: MAC Port Lockdown Theory of Operations **31**
2.1 Ethernet Port Security Components – Overview 31
2.2 MAC Port Lockdown for HP Switches – Scenarios Supported 33
2.2.1 Rules of Locking HP Switch Ports to Redundant Routers 34
2.3 MAC Port Lockdown for GCP 8000 Site Controllers and GPB 8000 Reference Distribution Modules – Scenarios Supported 34
2.4 Considerations When MAC Port Lockdown Is Enabled 35
2.5 Considerations for GCP 8000 Site Controller/GPB 8000 Reference Distribution Module Switch Settings 36
Chapter 3: MAC Port Lockdown Installation **37**
3.1 VoyenceControl Installation 37
3.2 Installing Mini-GBICs and Fiber Cables on HP 2620 Switches and HP 3500/3800 Switches 37
Chapter 4: MAC Port Lockdown Configuration **39**
4.1 Enabling MAC Port Lockdown 39

Chapter 5: MAC Port Lockdown Optimization..... 41

5.1 Optimization.....41

Chapter 6: MAC Port Lockdown Operation..... 43

6.1 MAC Port Lockdown – Operation Overview..... 43

6.2 Secure Protocol Considerations..... 43

6.3 Configuring MAC Port Lockdown for a Virtual Server with Redundant Switch Connections.....44

6.4 MAC Port Lockdown Procedures for GCP 8000 Site Controllers, GPB 8000 Reference Distribution Modules and XHubs – Overview..... 44

6.5 Viewing Ethernet Port Security for the GCP 8000 Site Controller and GPB 8000 Reference Distribution Module with CSS.....45

6.6 Capturing the MAC Address of a Device Connected to a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module.....46

6.7 Enabling/Disabling 802.1x and MAC Port Lockdown for GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with CSS.....47

6.8 Enabling/Disabling MAC Port Lockdown on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with Site Wizards.....49

6.9 Validating MAC Port Lockdown on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module.....50

6.9.1 Methods for Verifying MAC Port Lockdown on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module.....50

6.10 Unlocking/Locking the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module Ethernet Port When Replacing a Site Gateway.....51

6.11 MAC Port Lockdown Procedures for HP Switches – Overview.....52

6.12 Performing MAC Port Lockdown on HP Switches.....52

6.13 HP Switches – Accessing the Console Interface.....54

6.13.1 Accessing the HP Switch Console with Telnet or SSH.....55

6.13.2 Establishing Direct Console Access to the HP Switch.....55

6.14 Logging on to an HP Switch with Cut-Through.....56

6.15 Logging out of an HP Switch with Cut-Through.....57

6.16 Displaying HP Switch Port Status – Overview.....57

6.17 Displaying Port Security for HP Switches with a Saved Command.....57

6.18 Determining the Number of MAC Addresses Learned by a Port.....59

6.19 Locking HP Switch Ports with a VoyenceControl Template..... 60

6.20 Locking HP Switch Ports..... 61

6.21 Locking MAC Ports on HP Switches in Redundant Site-Link Configurations..... 62

6.22 Guide to Locking MAC Ports on HP Switches in Redundant Site-Link Configurations..... 65

6.23 Validating MAC Port Lockdown on HP Switches.....68

6.24 Disabling MAC Port Lockdown with Cut-Through in VoyenceControl..... 69

6.25 Disabling MAC Port Lockdown with a VoyenceControl Template..... 70

6.26 Disabling MAC Port Lockdown with an HP Switch Service Port.....71

6.27 Changing the Address Limit on a Previously Configured HP Switch Port..... 71

Chapter 7: MAC Port Lockdown Maintenance..... 73

7.1 Monitoring for Alarms and Re-Locking Ports..... 73

7.2 Software Patch Installation..... 73

Chapter 8: MAC Port Lockdown Troubleshooting..... 75

8.1 Fault Management for MAC Port Lockdown on HP Switches..... 75

8.1.1 UEM Alarms for MAC Port Lockdown on HP Switches..... 75

8.1.2 Centralized Event Logging for HP Switch Port Security..... 75

8.2 Viewing Centralized Event Logging Records for GCP 8000 Site Controller/GPB 8000 Reference Distribution Module Port Security..... 75

8.3 MAC Port Lockdown Faults..... 77

8.4 Link Failures..... 77

Chapter 9: MAC Port Lockdown FRU/FRE Recovery Procedures..... 79

9.1 Unlocking/Locking HP Switch Ports When Replacing Connected Devices..... 79

9.2 Locking/Unlocking a GCP 8000 Site Controller, GPB 8000 Reference Distribution Module or XHub Port When Replacing a Connected Device..... 80

9.3 Fiber Connections Between HP Switches – Field Replaceable Units..... 80

9.4 Mini-GBICs on HP 2620 and HP 3500/3800 Switches..... 81

9.5 Replacing Mini-GBICs on HP 2620 and HP 3500/3800 Switches..... 82

Chapter 10: MAC Port Lockdown Reference..... 85

10.1 Disabling 802.1x on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module Ethernet Port with the Serial Port..... 85

10.2 Enabling/Disabling Ports on HP Switches with Local Access..... 86

10.3 Enabling/Disabling Ports on HP Switches with VoyenceControl..... 87

10.4 Using a Motorola Solutions Template in VoyenceControl..... 87

10.5 Logging into VoyenceControl..... 88

10.6 Accessing the Configlet Editor in VoyenceControl..... 88

10.7 Populating a Configlet with a Pre-Tested Template..... 89

10.8 Scheduling a Job in VoyenceControl..... 90

10.9 Viewing the Job Status in VoyenceControl..... 92

10.10 Viewing a Configuration Change in VoyenceControl..... 92

10.11 Viewing Enabled/Disabled State for HP Switch Ports with a Saved Command..... 93

This page intentionally left blank.

List of Figures

Figure 1: GCP 8000 Site Controller Module..... 26
Figure 2: GPB 8000 Reference Distribution Module..... 27
Figure 3: Example of Ethernet Ports on HP 3500yl Switch (48-Port)..... 27
Figure 4: Example of Ethernet Ports on HP 3800 Switch (48-Port).....28
Figure 5: Example of Serial (Console) Port on HP 3500yl Switch (48-Port).....28
Figure 6: Example of Ethernet Ports on HP 2620 Switch.....28
Figure 7: HP Switch Mini-GBIC Transceiver..... 29
Figure 8: HP 2620 Switch – Ethernet Ports and Slots for GBICs..... 29
Figure 9: HP 3500 Switch – Ethernet Ports and Slots for GBICs..... 30
Figure 10: HP 3800 Switch – Ethernet Ports and Slots for GBICs..... 30
Figure 11: Single Zone Non-Redundant Master Site Components..... 32
Figure 12: Single Zone Redundant Master Site Components..... 32
Figure 13: Multi-Zone Capable Master Site Components..... 33
Figure 14: CSS Site Controller Switch Window – Local Switch Tab..... 45
Figure 15: CSS Site Controller Switch Window – Expansion Port Configuration Area..... 46
Figure 16: CSS Site Controller Switch Window – Port Security Menu..... 48
Figure 17: CSS Site Controller Switch Window – Expansion Port Security Menu..... 48
Figure 18: CSS Site Controller Switch Window – XHub Port Security Menu..... 48
Figure 19: HP Switch Mini-GBIC Transceiver..... 81
Figure 20: HP Switch Fiber Cable..... 81
Figure 21: HP 2610 Switch – Ethernet Ports and Slots for GBICs..... 81
Figure 22: HP 3500 Switch – Example of Ethernet Ports and Slots for GBICs..... 82
Figure 23: HP 3800 Switch – Example of Ethernet Ports and Slots for GBICs..... 82
Figure 24: VoyenceControl Configlet Editor Window – Example..... 89
Figure 25: VoyenceControl Schedule Job Window – Example..... 91
Figure 26: Schedule Manager Window – Example..... 92

This page intentionally left blank.

List of Tables

Table 1: MAC Port Lockdown for HP Switches – Supported Scenarios and Methods.....33
Table 2: MAC Port Lockdown for GCP 8000 Site Controllers and GPB 8000 Reference Distribution Modules – Supported Scenarios and Methods.....34
Table 3: Methods for Verifying MAC Port Lockdown on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with Ethernet Cables Swapped.....50
Table 4: Template Information to Lock HP Switch Ports.....60
Table 5: Guide to Locking MAC Ports on HP Switches in Redundant Site-Link Configurations.....65
Table 6: Template Information to Disable Port Security.....70
Table 7: Software Patches and References.....73
Table 8: System Events for GCP 8000 Site Controller/GPB 8000 Reference Distribution Module.....76
Table 9: Fiber Connections Between HP Switches – Field Replaceable Units.....80
Table 10: Template Information to Enable/Disable Unused Ports on HP Switches.....87

This page intentionally left blank.

List of Processes

Validating MAC Port Lockdown on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module 50

Unlocking/Locking the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module Ethernet Port When Replacing a Site Gateway 51

Performing MAC Port Lockdown on HP Switches 52

Using a Motorola Solutions Template in VoyenceControl 87

This page intentionally left blank.

List of Procedures

Installing Mini-GBICs and Fiber Cables on HP 2620 Switches and HP 3500/3800 Switches 37
Configuring MAC Port Lockdown for a Virtual Server with Redundant Switch Connections 44
Viewing Ethernet Port Security for the GCP 8000 Site Controller and GPB 8000 Reference Distribution Module with CSS 45
Capturing the MAC Address of a Device Connected to a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module 46
Enabling/Disabling 802.1x and MAC Port Lockdown for GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with CSS 47
Accessing the HP Switch Console with Telnet or SSH 55
Establishing Direct Console Access to the HP Switch 55
Logging on to an HP Switch with Cut-Through 56
Logging out of an HP Switch with Cut-Through 57
Displaying Port Security for HP Switches with a Saved Command 57
Determining the Number of MAC Addresses Learned by a Port 59
Locking HP Switch Ports 61
Locking MAC Ports on HP Switches in Redundant Site-Link Configurations 62
Validating MAC Port Lockdown on HP Switches 68
Disabling MAC Port Lockdown with Cut-Through in VoyenceControl 69
Disabling MAC Port Lockdown with an HP Switch Service Port 71
Changing the Address Limit on a Previously Configured HP Switch Port 71
Unlocking/Locking HP Switch Ports When Replacing Connected Devices 79
Replacing Mini-GBICs on HP 2620 and HP 3500/3800 Switches 82
Disabling 802.1x on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module Ethernet Port with the Serial Port 85
Enabling/Disabling Ports on HP Switches with Local Access 86
Logging into VoyenceControl 88
Accessing the Configlet Editor in VoyenceControl 88
Populating a Configlet with a Pre-Tested Template 89
Scheduling a Job in VoyenceControl 90
Viewing a Configuration Change in VoyenceControl 92
Viewing Enabled/Disabled State for HP Switch Ports with a Saved Command 93

This page intentionally left blank.

About MAC Port Lockdown

This manual describes the technical solution for MAC Port Lockdown on switch ports in ASTRO® 25 systems.

What is Covered In This Manual?

The following chapters are provided:

- MAC Port Lockdown Description on page 23, provides an overview of Ethernet Port Security and MAC Port Lockdown.
- MAC Port Lockdown Theory of Operations on page 31, describes how MAC Port Lockdown works in the context of your system.
- MAC Port Lockdown Installation on page 37, describes installation of the MAC Port Lockdown components.
- MAC Port Lockdown Configuration on page 39, provides procedures required to allow the feature to be programmed and function properly.
- MAC Port Lockdown Optimization on page 41, provides information about configurations for optimal performance.
- MAC Port Lockdown Operation on page 43, provides the system-level operating procedures for MAC Port Lockdown.
- MAC Port Lockdown Maintenance on page 73, lists information that may be required for maintenance of the MAC Port Lockdown feature.
- MAC Port Lockdown Troubleshooting on page 75, provides fault management and troubleshooting information related to the MAC Port Lockdown feature.
- MAC Port Lockdown FRU/FRE Recovery Procedures on page 79, includes a table of part numbers for Field Replaceable Units and Field Replaceable Entities, as well as replacement procedures.
- MAC Port Lockdown Reference on page 85, provides instructions that are useful when performing MAC Port Lockdown procedures in this manual. The information in this chapter is covered in more detail in other manuals.

Helpful Background Information

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to http://www.motorolasolutions.com/training.

Related Information

Refer to the following documents for associated information about the radio system.

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as R56 manual.

Table continued…

Related Information	Purpose
	This may be purchased on CD **9880384V83**, by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
System Overview and Documentation	Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system.
802.1x Service Ports on Switches manual	Provides information about setting up 802.1x on the service ports on switches and authenticating through the 802.1x port.
System LAN Switches manual	Provides use of Hewlett-Packard (HP) switches in ASTRO® 25 systems, including LAN switches and backhaul switches. In addition to common procedures for installation, configuration, operation, and troubleshooting of the switches, this manual provides information for specific ASTRO® 25 system sites and features that HP switches can support.

Chapter 1

MAC Port Lockdown Description

This chapter provides a functional description and an overview of the Media Access Control (MAC) Port Lockdown security feature.

1.1 Ethernet Port Security

This manual provides information about the Ethernet Port Security features available for switches in ASTRO® 25 systems. The Ethernet Port Security features do not change the system-level operation. They influence the internal operation of the Ethernet switches.

Two methods for Ethernet Port Security are available:

MAC Port Lockdown
Prevents unauthorized access to a system through a port on a network device by locking the port to one or more MAC addresses.

802.1x for Service Ports
Uses 802.1x standards to authenticate service users at designated ports.

NOTICE: This manual addresses **port-level** network access. For authentication at the device level, see the *Authentication Services* manual.
This manual can be used to support MAC Port Lockdown for the HP 2600 series switches at a K core or Conventional Hub Site in an ASTRO® 25 Conventional & Integrated Data System. Only references in this manual to the HP 2600 series switches apply to implementation of Ethernet port security for these switches used in an ASTRO® 25 Conventional & Integrated Data System.

1.2 MAC Port Lockdown

The Media Access Control (MAC) Port Lockdown feature provides a layer of security at the physical location of the equipment. MAC Port Lockdown prevents unauthorized access to the system through ports on a network device (for example, a switch) by locking each port to one or more MAC addresses. Access to the system through a locked port is denied to any devices with MAC addresses not matching the address(es) locked to that port.

Benefits include:

- Information sent to the locked address cannot be hijacked and directed out to the port of an intruder.
- MAC Port Lockdown also controls address learning on the switch so that unauthorized MAC addresses cannot be learned.
- In ASTRO® 25 systems, MAC Port Lockdown can be used to prevent station movement at remote sites.

You cannot lock down a single MAC address to more than one port. If a device with a MAC address locked to a specific port on a switch is moved to a different port on the switch (by reconnecting the Ethernet cable), access to the system is denied to that device. The port will detect that the MAC Address is not on the appropriate port and will continue to send traffic out the port to which the address was locked.

Stations can move from the port to which their MAC address is locked to other parts of the network. They can send, but will not receive data if that data must go through the locked down switch.

NOTICE: If the device moves to a distant part of the network where data sent to its MAC address never goes through the locked down switch, it may be possible for the device to have full two-way communication.

1.3 Ethernet Port Security in ASTRO 25 Systems

In an ASTRO® 25 system, Ethernet Port Security is implemented by configuring standard 10/100Base-T Ethernet ports on:

- HP switches
- GCP 8000 Site Controller's internal switch
- GPB 8000 Reference Distribution Module

At least one of the following settings must be applied:

- **Disabled:** When no equipment is attached to a port.
- **Locked through MAC Port Lockdown:** When a port is permanently connected and is set up to a network element such as a network router.

  NOTICE: MAC Port Lockdown cannot be applied to redundant routers at:

  - ASTRO® 25 Repeater Sites with GTR 8000 Base Radios
  - IP Simulcast remote subsites

    NOTICE: For the IP Simulcast prime sites with geographical redundancy enabled, fiber ports are not enabled.

  The MAC Port Lockdown and 802.1x features are not supported on the conventional GCP 8000 Site Controller or on the GCM 8000 Comparator.
- **Configured for 802.1x Port Security:** When a port is reserved for a service user. With this setting, the service user computer can only gain access, when the service user enters the correct credentials.

In order to achieve this result, Motorola Solutions provides the following:

- **Customized system configuration plan:** A plan that documents the port connections for each device.
- **Configuration tools:** tools that can display, set, back up, and restore the port state of every Ethernet port on switches where port security is implemented. These tools can also be used to view the configuration for each switch where MAC Port Lockdown is implemented, to see what connects to each port on the switch.

  NOTICE: See the *Unified Network Configurator* manual, and *CSS Online Help*.
- **Remote Authentication Dial-In User Service (RADIUS):** This service has the capability for authenticating users of 802.1x ports.

  NOTICE: In order to support service port security, RADIUS must be set up on the domain controllers, and must maintain accounts for service users and shared keys for 802.1x-enabled devices. For more information, see the *Authentication Services* manual.

1.3.1

Switches Supporting Ethernet Port Security in ASTRO 25 System

The following switches in an ASTRO® 25 system support the Ethernet Port Security feature:

HP switches at the Master Site:

- Core Local Area Network (LAN) switch
- Mediation LAN switch, if Zone Core Protection (ZCP) is implemented in the system
- Intrusion Detection System (IDS) switch, if ZCP is implemented in the system and an IDS sensor is set up to monitor traffic from the ZCP Mediation LAN switch, as well as the DMZ switch

Additional HP switches, if these sites are present in the system:

- Network Management Dispatch Site switch
- Simulcast Remote Site
- Simulcast Prime Site
- HPD Overlay Site
- Backhaul Switches (if required)
- RF Conventional Site with a multiple site gateway (conventional channel interface) configuration
- Conventional Base Radio Site
- Conventional Hub Site
- Geographically Redundant Prime Site

NOTICE: For information on Backhaul Switches, refer to the *System LAN Switches* manual.

Internal switch on GCP 8000 Site Controllers, GPB 8000 Reference Distribution Module and Expansion Hubs at the following sites, if these sites are present in the system:

- Repeater Sites with GTR 8000 Base Radios
- HPD Standalone Site
- IP Simulcast high availability remote subsite

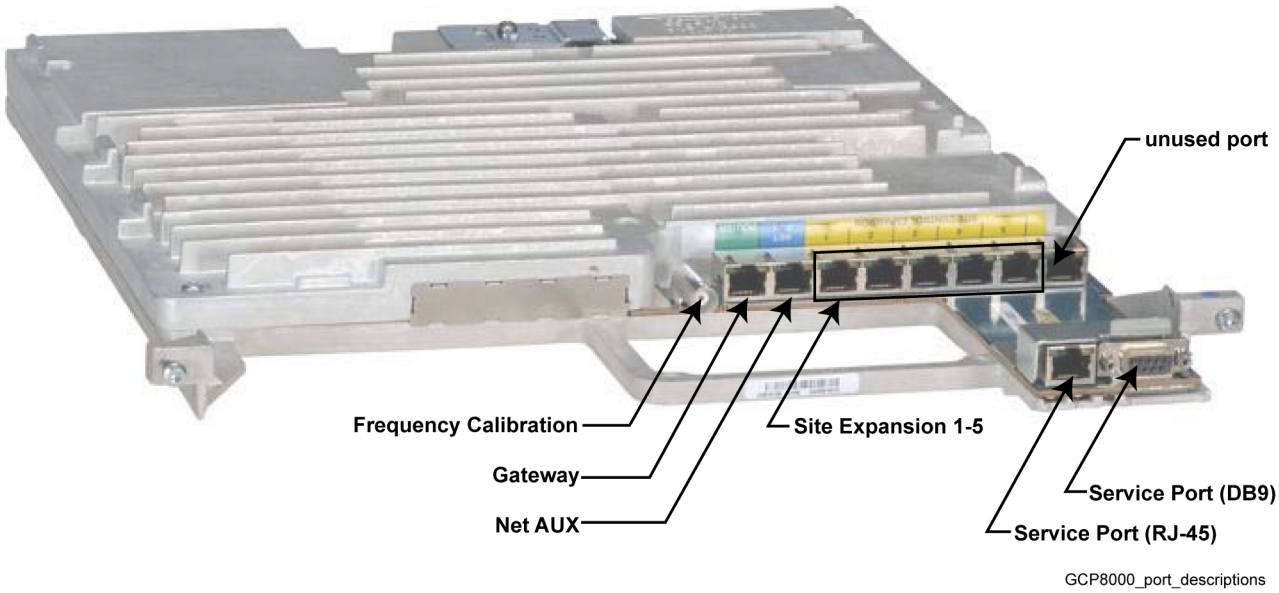
NOTICE: MAC Port Lockdown cannot be applied to the switch ports connected to redundant routers at ASTRO® 25 Repeater Sites with GTR 8000 Base Radios and IP Simulcast remote subsites.

1.4

Location of Ports on the GCP 8000 Site Controller

Figure 1: GCP 8000 Site Controller Module

The following figure shows an example of a GCP 8000 Site Controller. GCP 8000 Site Controllers are used at ASTRO® 25 repeater sites and simulcast prime sites.



The 802.1x feature can be implemented on the Ethernet (RJ-45) Service Port on the GCP 8000 Site Controller internal switch. MAC Port Lockdown can be implemented on the other Ethernet ports on the GCP 8000 Site Controller internal switch. Additionally, MAC Port Lockdown can be implemented on the internal switch ports of Expansion Hubs that may be connected to a GCP 8000 Site Controller.

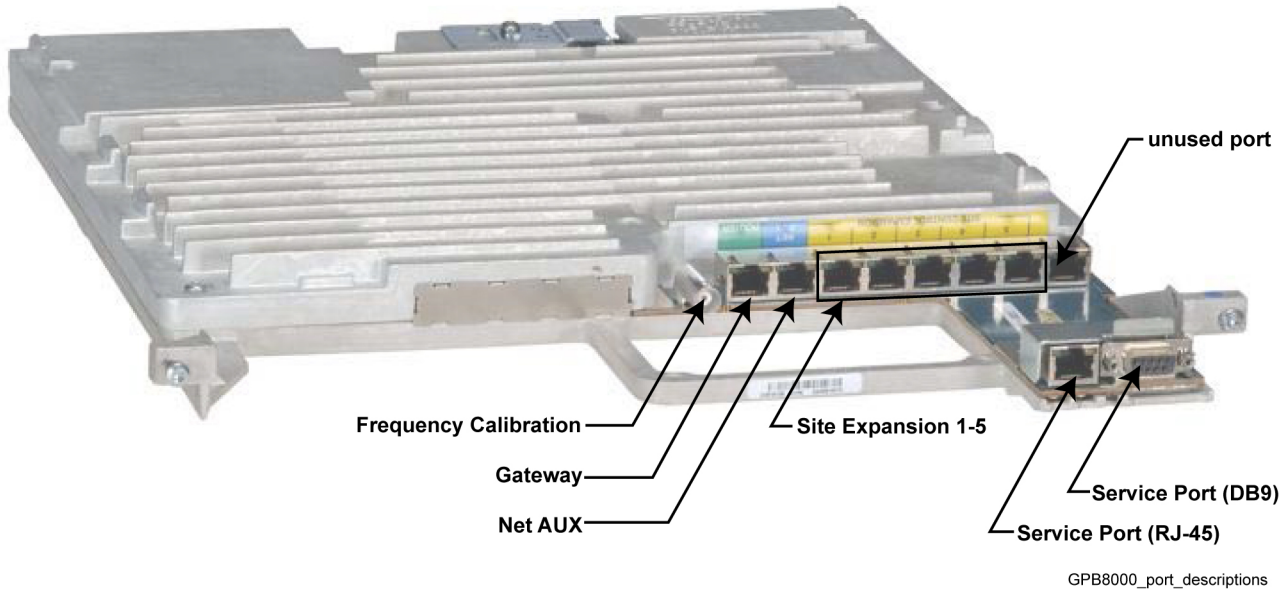
For more information about these devices and sites, refer to the ASTRO® 25 system manuals about the sites which use GCP 8000 Site Controllers.

1.5

Location of Ports on the GPB 8000 Reference Distribution Module

Figure 2: GPB 8000 Reference Distribution Module

The following figure shows an example of a GPB 8000 Reference Distribution Module. GPB 8000 Reference Distribution Modules are used at remote RF sites.



The 802.1x feature can be implemented on the Ethernet (RJ-45) Service Port on the GPB 8000 Reference Distribution Module internal switch. MAC Port Lockdown can be implemented on the other Ethernet ports on the GPB 8000 Reference Distribution Module internal switch. Additionally, MAC Port Lockdown can be implemented on the internal switch ports of Expansion Hubs that may be connected to a GPB 8000 Reference Distribution Module.

For more information about these devices and sites, refer to the ASTRO® 25 system manuals about the sites which use GPB 8000 Reference Distribution Modules.

1.6

Location of Ports on HP Switches

The following figures in this section show the location of Ethernet ports and the serial console port on a Master Site LAN switch.

Figure 3: Example of Ethernet Ports on HP 3500yl Switch (48-Port)

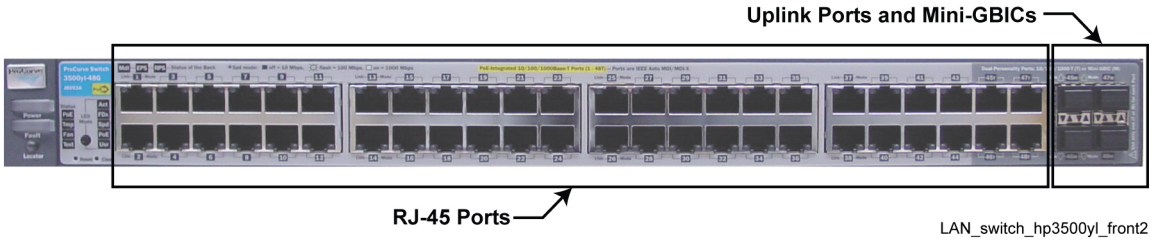
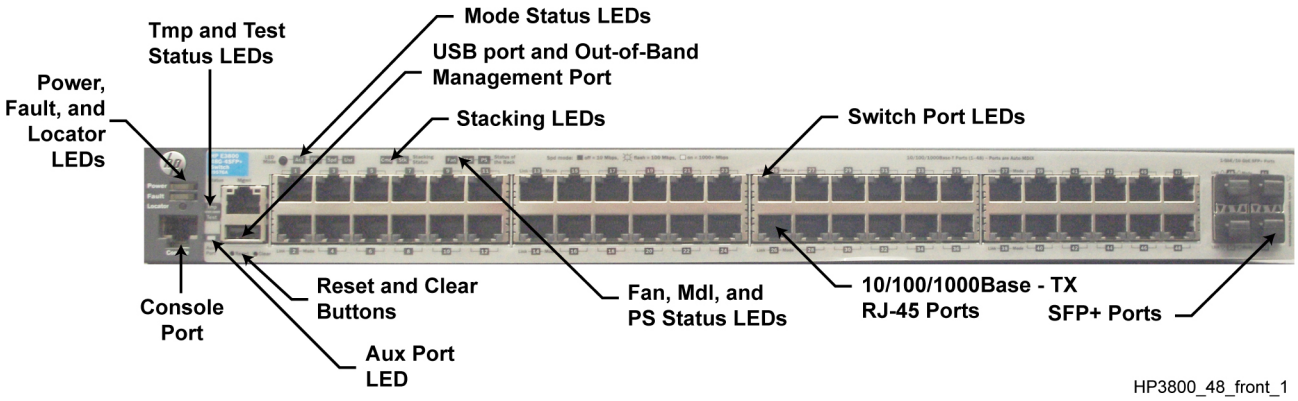


Figure 4: Example of Ethernet Ports on HP 3800 Switch (48-Port)



NOTICE: For features and specifications of HP 3800-48 switches, see the “HP 3800 Switches – Common Information” chapter in the *System LAN Switches* manual.

Figure 5: Example of Serial (Console) Port on HP 3500yl Switch (48-Port)

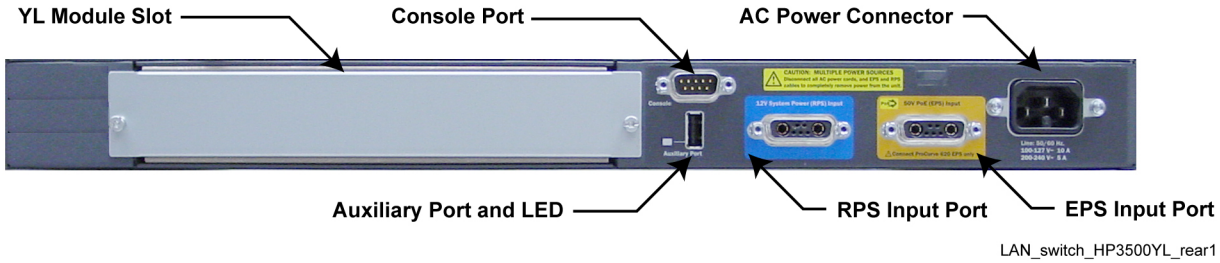
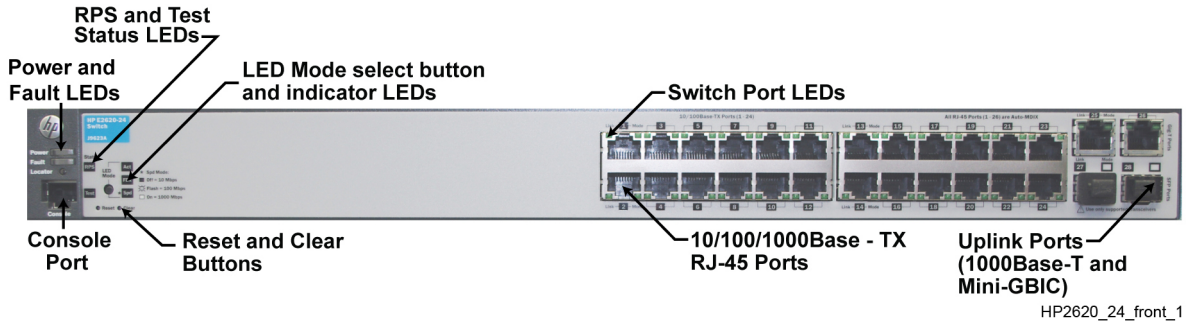


Figure 6: Example of Ethernet Ports on HP 2620 Switch

The following figure shows that the HP 2610 and HP 2620 switches have the same Ethernet port configurations, despite visual differences.



MAC Port Lockdown and 802.1x can be implemented on the Ethernet ports of these switches. The serial port may be needed for local access when configuring the Ethernet ports.

NOTICE: There is no specific Ethernet port designated as the standard service port on HP switches in ASTRO® 25 systems. Consult your system configuration plan when selecting an HP switch port to use as an 802.1x-enabled service port.
The mesh ports of 24-port HP 3500 switches installed in a mesh configuration at Simulcast Prime Sites do not support the MAC Port Lockdown feature. However, MAC Port Lockdown is still supported on the ports not involved in the mesh.

1.7

Additional Security with Fiber Optic Ports

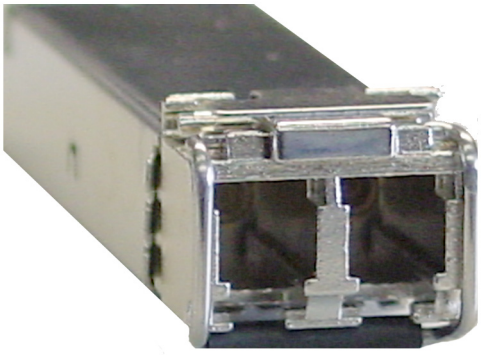
Fiber optic ports provide additional security when connecting HP switches (if more than one switch is installed at a site), and the ports for connecting the HP switches would otherwise be 1000BaseT copper ports. Fiber optic ports can be provided in mini-Gigabit Interface Cards (mini-GBICs). If a mini-GBIC or the fiber optic cable is removed, faults are generated and reported to the fault management system, thus providing a level of local port security.

NOTICE: It is recommended that mini-GBICs be used when connecting two HP switches and the ports for connecting the HP switches would otherwise be 1000BaseT copper ports.

When a mini-GBIC transceiver is inserted into the slot provided for it on a switch, that port is enabled and the associated 1000BaseT port is disabled.

NOTICE: If the mini-GBIC is removed, the associated Ethernet port is automatically re-enabled; however, the Ethernet port is not configured to connect to the network. If the mini-GBIC has been removed and the switch reboots, the trunked ports are assigned to their default Virtual LAN (VLAN). The only way to connect to the network in this case is to re-insert the mini-GBICs and reload the switch configuration, that re-assigns the fiber optic ports to the trunking configuration.

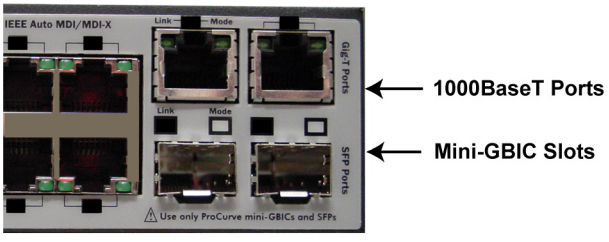
Figure 7: HP Switch Mini-GBIC Transceiver



HP_Switch_GBIC_Transceiver

Figure 8: HP 2620 Switch – Ethernet Ports and Slots for GBICs on page 29 shows the two slots where the mini-GBICs are inserted in the HP 2620 switch and the two 1000BaseT Ethernet ports that are automatically disabled when the mini-GBICs are inserted.

Figure 8: HP 2620 Switch – Ethernet Ports and Slots for GBICs



Switch_HP2610_GBIC1

HP 3500/3800-48 switches also include slots for mini-GBICs, located to the right of the associated BaseT copper ports.

Figure 9: HP 3500 Switch – Ethernet Ports and Slots for GBICs on page 30 shows the slots where mini-GBICs can be inserted on an HP 3500 switch and the associated 1000BaseT Ethernet ports.

Figure 9: HP 3500 Switch – Ethernet Ports and Slots for GBICs

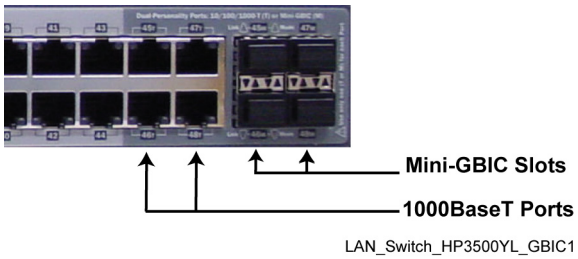
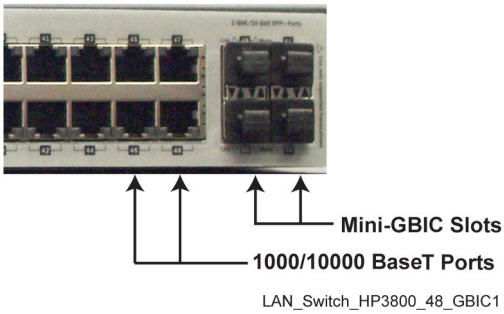


Figure 10: HP 3800 Switch – Ethernet Ports and Slots for GBICs on page 30 shows the slots where mini-GBICs can be inserted on an HP 3800-48 switch and the associated 1000/10000BaseT Ethernet ports. Inserting mini-GBICs into the slots creates SFP+ (fiber) ports.

Figure 10: HP 3800 Switch – Ethernet Ports and Slots for GBICs



NOTICE: HP 3800 ports do not have dual personality. The ILO Out-of-Band Management Port is automatically disabled in the ASTRO® 25 system switch configuration.

In an ASTRO® 25 system, mini-GBIC slots 47M and 48M are used when implementing fiber ports for two trunked HP 3500 switches. This disables the associated 1000BaseT ports (ports 47T and 48T).

Similarly, in an ASTRO® 25 system, 51 and 52 mini-GBIC slots are used when implementing fiber ports for two trunked HP 3800 switches.

NOTICE: The mini-GBIC ports always operate at full duplex.

For a geographically redundant prime site, fiber ports are not supported. The LAN switch demarcation point is the copper based ports. Using fiber backhaul for the intra-prime site links requires customer-provided media converters to interface with the LAN switch copper ports.

Chapter 2

MAC Port Lockdown Theory of Operations

This chapter explains how Ethernet Port Security works in the context of your system.

2.1 Ethernet Port Security Components – Overview

This section provides a brief overview of the system components, which support Ethernet Port Security in an ASTRO® 25 system.

Depending on your organization's needs, Motorola Solutions provides the following configurations:

- Single Zone Non-Redundant
- Single Zone Redundant
- Multi-Zone Capable

Figure 11: Single Zone Non-Redundant Master Site Components on page 32, Figure 12: Single Zone Redundant Master Site Components on page 32, and Figure 13: Multi-Zone Capable Master Site Components on page 33 show **master site redundant routers**. These routers connect to switch ports which require a unique process for implementing MAC Port Lockdown, so that the inactive router becomes active before MAC addresses are learned.

In each of those configurations, the following zone core components support Ethernet Port Security in an ASTRO® 25 system:

Master site Ethernet LAN switches
These are examples of switches where Ethernet Port Security is implemented.

Domain Controllers (DCs)
The DCs host the RADIUS service required for 802.1x port security (for more information, see the *Authentication Services* manual).

Unified Network Configurator (UNC) application
The UNC application hosts the centralized configuration tool used to set up port security.

NOTICE: Depending on the Master Site configuration, the number of switches, routers, and Domain Controllers varies.
Backhaul Switches may be present in the system, if required. They provide infrastructure to support for fault management of PTP Wireless Ethernet Bridges in an ASTRO® 25 system. MAC Port Lockdown procedures can be implemented on these switches. For more details regarding the feature supporting fault management of PTP devices in an ASTRO® 25 system, see the *Fault Management – System Perspective* manual. For more information on Ethernet LAN Switches, see the *System LAN Switches* manual.

For PTP implementation using the Extreme Networks E4G Series Switch, contact the Extreme Networks or Cambium Networks field representative.

Figure 11: Single Zone Non-Redundant Master Site Components

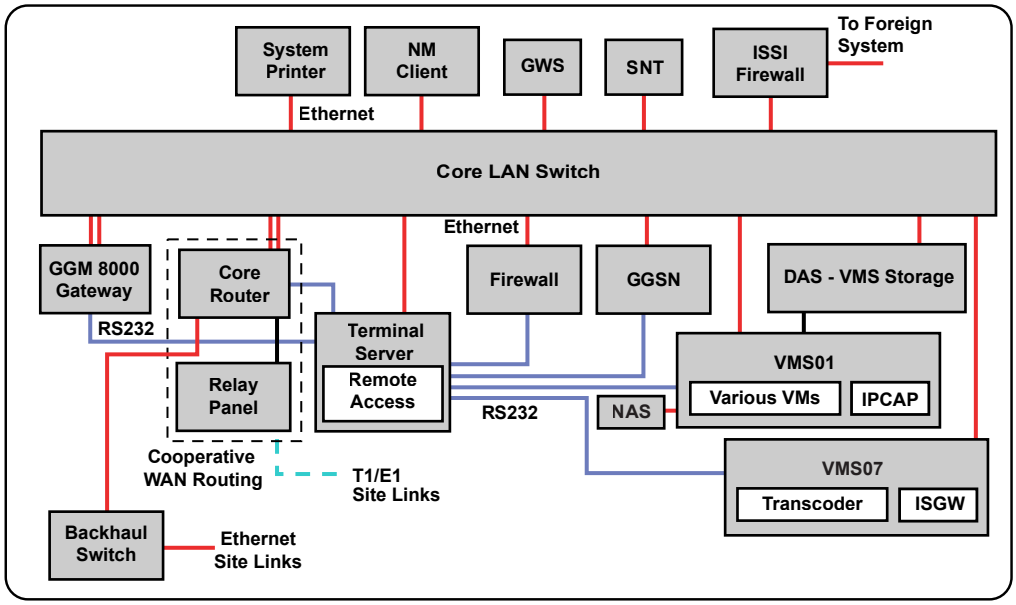


Figure 12: Single Zone Redundant Master Site Components

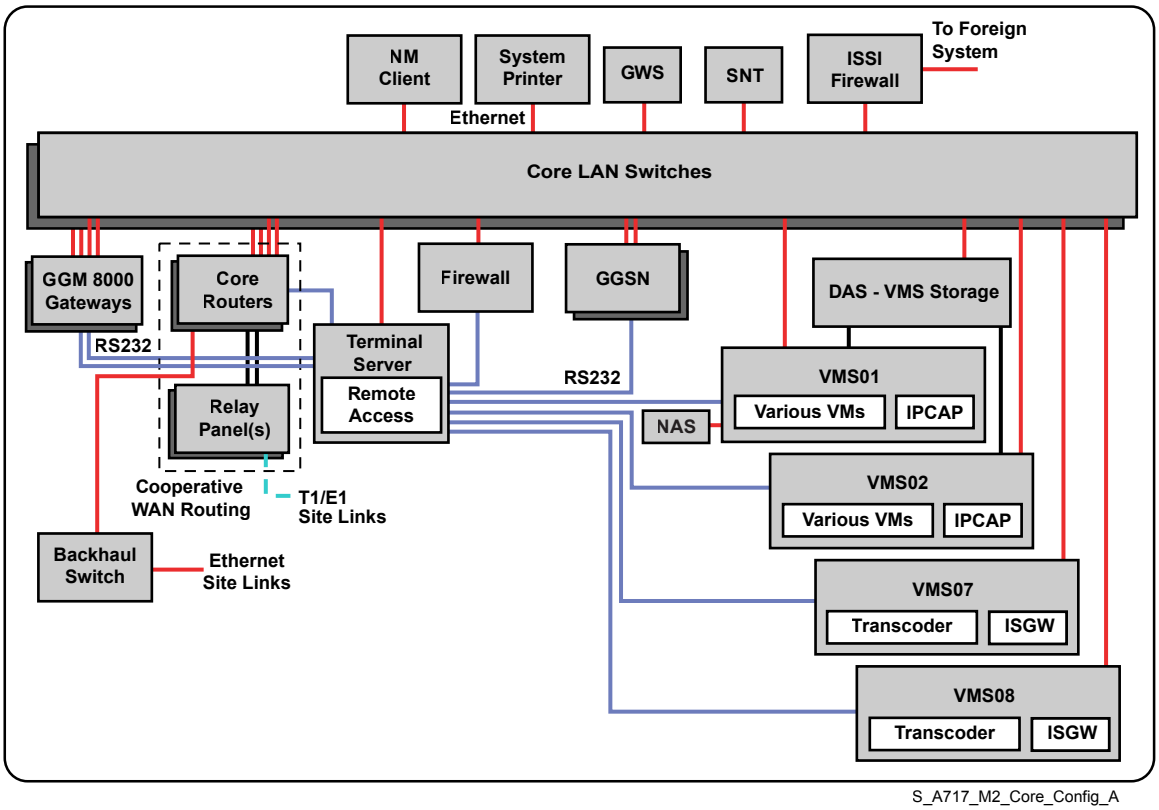
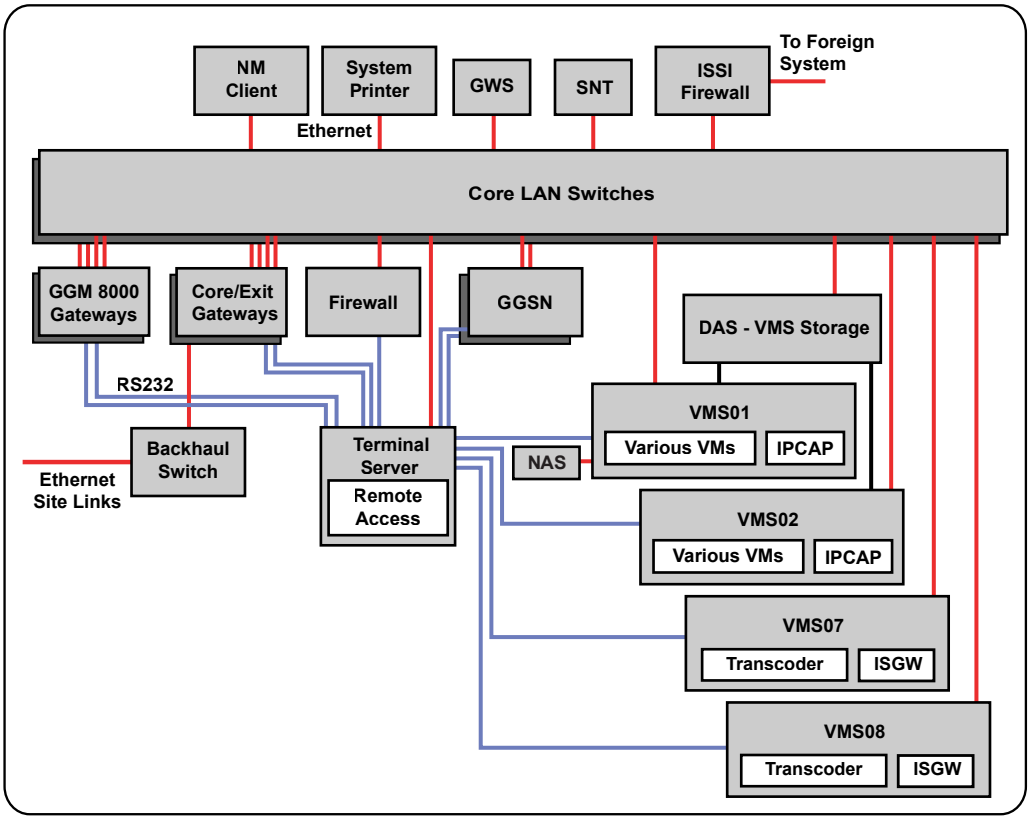


Figure 13: Multi-Zone Capable Master Site Components



S_A717_M3_Primary_System_Zone_Core_Config_A

For a diagram and details of LAN Switches in a geographically redundant prime site, see the *System LAN Switches* manual.

2.2

MAC Port Lockdown for HP Switches – Scenarios Supported

Before performing MAC Port Lockdown on an HP switch, see the following table to determine which of the scenarios applies. Then, see MAC Port Lockdown Operation on page 43 for the procedure which supports that scenario.

Table 1: MAC Port Lockdown for HP Switches – Supported Scenarios and Methods

Scenarios Supported	Methods Available
Locking/Unlocking an HP switch port or ports to a single MAC address	HP switch command line, accessed locally **or, if network access is available:** VoyenceControl template
Locking/Unlocking an HP switch port or ports to multiple MAC addresses	or VoyenceControl Cut-Through to the HP switch command line **NOTICE:** The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

Table continued…

Scenarios Supported	Methods Available
Locking/Unlocking an HP switch port to the MAC address for a redundant router	HP switch command line, accessed locally **or, if network access is available:** VoyenceControl Cut-Through to the HP switch command line (VoyenceControl templates support this scenario. However, the command line may be a more convenient method.) **NOTICE:** The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

NOTICE: The scenarios listed above require determining the number of MAC addresses that the port has learned as part of its operation within the current system configuration (after MAC Port Lockdown is performed, the port will be unable to learn any additional MAC addresses).

2.2.1
Rules of Locking HP Switch Ports to Redundant Routers

If there are two routers connected to the Ethernet ports on the switches, and MAC Port Lockdown needs to be performed on each of these Ethernet ports, the MAC Port Lockdown procedure needs to include switching the inactive router to become the active router in a proper sequence.

For example, if the first router is connected to port 1 of the first switch, and the second router is connected to port 2 of the second switch, port security is first enabled on port 1 of the first switch. The first router is then rebooted so that the second router (inactive router) becomes the active router. The port security is then enabled on port 2 of the second switch.

In Single Zone Non-Redundant configuration, there is only one switch and no redundant routers. Therefore, MAC Port Lockdown needs to be performed only once.

The same rule applies for each of the prime sites in a geographically redundant configuration.

2.3
MAC Port Lockdown for GCP 8000 Site Controllers and GPB 8000 Reference Distribution Modules – Scenarios Supported

Before performing MAC Port Lockdown on the internal switch of a GCP 8000 Site Controller and GPB 8000 Reference Distribution Module at a remote RF site, see the following table to determine which of the scenarios applies. Then, see MAC Port Lockdown Operation on page 43 for the procedure which supports that scenario.

Table 2: MAC Port Lockdown for GCP 8000 Site Controllers and GPB 8000 Reference Distribution Modules – Supported Scenarios and Methods

Scenarios Supported	Methods Available
Locking/Unlocking the Ethernet ports on the GCP 8000 Site Controllers and GPB 8000 Reference Distribution Modules at the remote site (except the ports connected to routers)	Use the **MAC Port Lockdown State** field in the Site Configuration Wizard for RF sites. This wizard is available in the ASTRO® 25 system centralized configuration tool. See the *Unified Network Configurator* manual for information.

Table continued…

Scenarios Supported	Methods Available
Locking/Unlocking all the Ethernet ports on any Expansion Hubs (XHubs) connected to the GCP 8000 Site Controllers or GPB 8000 Reference Distribution Modules at the remote site	
Locking/Unlocking an individual Ethernet port on a GCP 8000 Site Controller and GPB 8000 Reference Distribution Module or any of the XHubs connected to that GCP 8000 Site Controller or GPB 8000 Reference Distribution Module	Configuration of Port Security for individual ports is available in the Configuration/Service Software (CSS) application. However, this method should be used with caution. See Considerations for GCP 8000 Site Controller/GPB 8000 Reference Distribution Module Switch Settings on page 36. **NOTICE:** In the Configuration/Service Software (CSS) application, the window name is **Site Controller Switch** for GCP 8000 Site Controller, and **Switch Configuration** for GPB 8000 Reference Distribution Module. Also, note that the switch ports connected to redundant routers at ASTRO® 25 Repeater Sites with GTR 8000 Base Radios cannot be locked. The MAC Port Lockdown feature, when implemented on the GCP 8000 Site Controller/GPB 8000 Reference Distribution Module Gateway ports, is not compatible with the redundancy protocol used with redundant Site Gateways. The redundancy protocol used relies on sharing a MAC address on the redundant gateways. This would require the same MAC address to be present on multiple switch ports of the GCP 8000 Site Controller/GPB 8000 Reference Distribution Module, which is not supported.

2.4 Considerations When MAC Port Lockdown Is Enabled

After MAC Port Lockdown is enabled, the following factors apply:

- Notification of a security violation is sent to the Unified Event Manager (UEM) if an unauthorized device is connected to a MAC Port Lockdown enabled port on an HP switch. UEM notification is already set up as part of overall system configuration. Notification of a security violation is also sent to a Centralized Event Logging (Syslog) server if that feature is implemented. Refer to the procedures for disabling/enabling Centralized Event Logging on HP switches in the *Centralized Event Logging* manual.
- If the device assigned to a port is changed, MAC Port Lockdown needs to be performed to update the port with the new device's MAC address. For more information, see:
  - Unlocking/Locking HP Switch Ports When Replacing Connected Devices on page 79
  - Locking/Unlocking a GCP 8000 Site Controller, GPB 8000 Reference Distribution Module or XHub Port When Replacing a Connected Device on page 80
- For HP switches, relocking and re-enabling a port is required after an access attempt by a device with an unauthorized MAC address, because this automatically disables the port. You can view the

MAC address of an unauthorized device on an HP switch by entering the following at the command line at the switch. The following command displays the Port, MAC Address, and Date/Time:
`show port-security intrusion-log`

- For the GCP 8000 Site Controller or GPB 8000 RDM, traffic is blocked if a device with an unauthorized MAC address attempts access at a locked port, but the locked port is not disabled, so relocking and re-enabling a port is not required.

NOTICE: HP switch **port-security** commands are only used for MAC Port Lockdown functions, not 802.1x functions.

2.5 Considerations for GCP 8000 Site Controller/GPB 8000 Reference Distribution Module Switch Settings

For GCP 8000 Site Controller/GPB 8000 Reference Distribution Module internal switches, the port security state can be one of the following:

- Locked
- 802.1x
- No security

A port cannot be set to "802.1x" and "Locked" at the same time.

IMPORTANT:
For GCP 8000 Site Controller/GPB 8000 Reference Distribution Module internal switches, if “No security” is selected for one port, then the switch is **not** considered secure. This is true even if “Locked” or “802.1x” is selected for the other ports.

No port security settings, even if configured, are applicable when a port is disabled. When a disabled port is enabled, the port security must be set to "802.1x" or "Locked".

If no device is plugged into a port on the GCP 8000 Site Controller/GPB 8000 Reference Distribution Module, and if the port is configured to be "Locked," then that port is locked out. This means that the port is disabled and no device can communicate on the port.

If a device that is locked down to a port on a switch is moved to an 802.1x port on the same switch, the device will receive an error message and will not be allowed to authenticate.

Chapter 3

MAC Port Lockdown Installation

This chapter provides installation information related to the MAC Port Lockdown feature.

3.1 VoyenceControl Installation

Before Ethernet Port Security is implemented, the VoyenceControl component of Motorola's Unified Network Configurator (UNC) tool should be operating and maintaining up-to-date device configurations for HP switches, GCP 8000 Site Controllers, and GPB 8000 Reference Distribution Module. Refer to the *Unified Network Configurator* manual for information on installing this tool's server and client applications, configuring its users and settings, and managing devices.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

3.2 Installing Mini-GBICs and Fiber Cables on HP 2620 Switches and HP 3500/3800 Switches

Prerequisites:

- Obtain valid configuration files for the switches.
- Locate the IP address for TFTP Server. Contact your system administrator for this information.
- Ensure connectivity to the switches from a computer with a TFTP server. (For the secure equivalent of TFTP, refer to the *Securing Protocols with SSH* manual.)
- See Mini-GBICs on HP 2620 and HP 3500/3800 Switches on page 81 for considerations regarding Ethernet ports and mini-GBICs on HP switches.
- See the *System LAN Switches* manual for which Ethernet or Fiber ports to use when connecting HP switches.
  - **Mini-GBICs (SX-LC transceivers):** CLN8490A from the North America Parts Organization (two are required per switch)
  - **Multi-mode fiber cables - LC(M), 3.3 ft.:** CKN6906A from the North America Parts Organization (two are required if there are two switches)

When and where to use:
Mini-GBIC installation is only required for Ethernet Port Security when there are two or more HP 2620 switches, or two or more HP 3500/3800-48 switches in trunk configuration, and the ports for connecting the HP switches would otherwise be 1000BaseT copper ports.

When a single HP switch is present in the system, do not install the fiber optic ports. Since the fiber optics ports are not installed, the associated Ethernet ports can be disabled. See Enabling/Disabling Ports on HP Switches with VoyenceControl on page 87.

Procedure:

1. Remove the dust cover from the mini-GBIC slot, if present.

2 Hold the mini-GBIC by its sides and gently insert it into one of the slots on the switch until the mini-GBIC clicks into place.

   The LED on the associated 1000BaseT port turns off.

3 Repeat step 2 for all mini-GBICs.

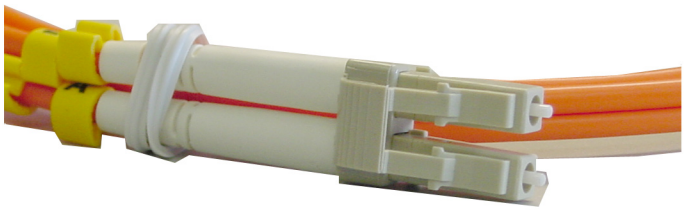
4 Reload the configuration to both switches using the following command:

   `copy tftp start <IP address of TFTP Server><config file name>`

   The configuration is loaded to the switch and the switch reboots.

5 Remove the dust covers from the fiber optic cable connectors, then connect one end of the fiber optic cable to a mini-GBIC port on one switch and the other end to the corresponding mini-GBIC port on another switch.

   See the *System LAN Switches* manual for a list of port connections.



HP_Switch_Fiber_Cable

NOTICE: After aligning the notches on the cable connectors with the slots on the port, be sure to press the cable connector into the port until it snaps into place.

   The corresponding link LEDs turn ON.

6 Repeat step 5 for the remaining ports on all of the trunked switches.

Chapter 4

MAC Port Lockdown Configuration

This chapter is for configuration procedures relating to MAC Port Lockdown.

4.1 Enabling MAC Port Lockdown

For the procedures to enable and disable MAC Port Lockdown, see MAC Port Lockdown Operation on page 43.

This page intentionally left blank.

Chapter 5

MAC Port Lockdown Optimization

This chapter is for optimization procedures and recommended settings related to MAC Port Lockdown.

5.1 Optimization

There are no optimization procedures required for the MAC Port Lockdown feature.

This page intentionally left blank.

Chapter 6

MAC Port Lockdown Operation

This chapter details tasks to perform after the MAC Port Lockdown feature is installed and operational on your system.

6.1 MAC Port Lockdown – Operation Overview

This chapter provides procedures for managing MAC Port Lockdown on the following hardware components of an ASTRO® 25 system:

- The internal switch of a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module. See MAC Port Lockdown Procedures for GCP 8000 Site Controllers, GPB 8000 Reference Distribution Modules and XHubs – Overview on page 44.
- HP switches. See MAC Port Lockdown Procedures for HP Switches – Overview on page 52.

The sections referenced above include procedures for enabling and disabling MAC Port Lockdown on an Ethernet port (locking and unlocking the ability of a port to learn new MAC addresses).

NOTICE: This chapter assumes that all prerequisite procedures have been completed. See the “Installation” and “Configuration” chapters of the manuals that are related to these features and hardware components.

Before performing any procedures using the VoyenceControl component of Motorola's Unified Network Configurator (UNC) application, VoyenceControl installation and initial client setup must be completed. You must have administrator privileges in VoyenceControl and access to VoyenceControl from a Network Management client. Also, the devices in the procedures need to be discovered in VoyenceControl and their configurations need to be recently pulled into VoyenceControl.

NOTICE: K core Conventional systems do not host a Unified Network Configurator (UNC). VoyenceControl and Cut-Through procedures do not apply. Use telnet/SSH or Direct Console procedures to access the switch. This manual can be used to support MAC Port Lockdown for the HP 2600 series switches at a K core or Conventional Hub Site in an ASTRO® 25 Conventional & Integrated Data System. Note that only references in this manual to the HP 2600 series switches will apply to implementation of Ethernet port security for these switches used in an ASTRO® 25 Conventional & Integrated Data System.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

6.2 Secure Protocol Considerations

Use the protocol permitted by your system configuration and security policies for procedures that require communication between VoyenceControl and a remote device, or other procedures that require remote network communications (for example, testing network connectivity).

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

For information about secure protocols, see the *SNMPv3* manual.

For additional information, refer to the *Securing Protocols with SSH* manual.

6.3

Configuring MAC Port Lockdown for a Virtual Server with Redundant Switch Connections

When and where to use: Follow these steps to configure MAC Port Lockdown for a virtual server with Redundant Connections. Virtual server MAC addresses are learnable only through the active connection of the virtual server. For redundancy, the MAC address of the virtual machine must be learned by all the switches. In case of failure of the primary switch or active connection, the redundant connection to the second core LAN switch is changed from standby to active.

NOTICE: This procedure only applies to M2 and M3 master site configurations. It does not apply to L2 master site configurations.

Procedure:

1. Unplug the first virtual server cable from its switch.
2. Perform the following for the other switch to learn its MAC addresses:
   a. From the HP switch, ping the IP address of the ESXi virtual server and of each virtual machine on the ESXi–based server.
   b. Perform Determining the Number of MAC Addresses Learned by a Port on page 59.
   c. Lock each used port. See Locking HP Switch Ports with a VoyenceControl Template on page 60.
3. Plug the first virtual server cable back into its switch.
4. Unplug the second virtual server cable from its switch.
5. Perform the following for the other switch to learn its MAC addresses:
   a. From the HP switch, ping the IP address of the ESXi virtual server and of each virtual machine on the ESXi–based server.
   b. Perform Determining the Number of MAC Addresses Learned by a Port on page 59.
   c. Lock each used port. See Locking HP Switch Ports with a VoyenceControl Template on page 60.

6.4

MAC Port Lockdown Procedures for GCP 8000 Site Controllers, GPB 8000 Reference Distribution Modules and XHubs – Overview

The following procedure is used to view whether MAC Port Lockdown is enabled on the Ethernet ports on the internal switch of a GCP 8000 Site Controller, GPB 8000 Reference Distribution Module or XHub in an ASTRO® 25 system:

- Viewing Ethernet Port Security for the GCP 8000 Site Controller and GPB 8000 Reference Distribution Module with CSS on page 45

The following procedures are used to enable/disable MAC Port Lockdown on the Ethernet ports on the internal switches of GCP 8000 Site Controllers, GPB 8000 RDMs and XHubs in an ASTRO® 25 system:

- Capturing the MAC Address of a Device Connected to a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module on page 46
- Enabling/Disabling 802.1x and MAC Port Lockdown for GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with CSS on page 47

- Enabling/Disabling MAC Port Lockdown on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with Site Wizards on page 49
- Validating MAC Port Lockdown on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module on page 50
- Unlocking/Locking the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module Ethernet Port When Replacing a Site Gateway on page 51

6.5 Viewing Ethernet Port Security for the GCP 8000 Site Controller and GPB 8000 Reference Distribution Module with CSS

Prerequisites: Obtain the following information from your system administrator:

- IP address of the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module you want to access
- Credentials for accessing the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module

When and where to use: Follow these steps to view Ethernet port security for a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module using the Configuration/Service Software (CSS).

Procedure:

1. Launch the **CSS** application.
2. Click the **Connect to Device** button in the toolbar, or go to **Tools** → **Connection Configuration**.

   The Connection screen appears.
3. Enter the ***<IP address>*** of the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module you want to access and click **Connect**.

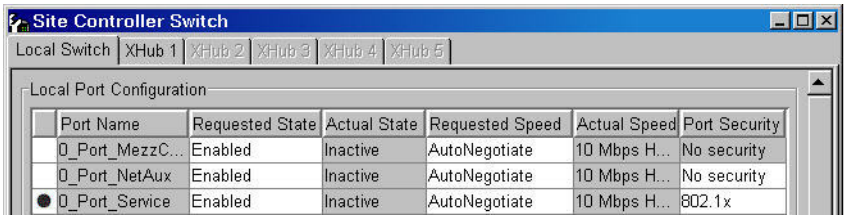
   If an authentication window appears, enter your credentials.

   A message states that CSS is successfully connected to the device.
4. Go to **File** → **Read Configuration from Device**.

   The Connection screen appears.
5. In the navigation pane on the left, select one of the following:
   - For GCP 8000 Site Controller, select **Site Controller Switch**.
   - For GPB 8000 Reference Distribution Module, select **Switch Configuration**.

   The following window displays.

   Figure 14: CSS Site Controller Switch Window – Local Switch Tab



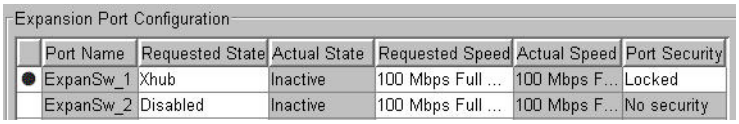
6 To view details, including the Port Security settings, perform one of the following:

- For GCP 8000 Site Controller, in the **Site Controller Switch** window, select the **Local Switch** tab.
- For GPB 8000 Reference Distribution Module, in the **Switch Configuration** window, select the **Local Switch** tab.

Postrequisites:

- If Expansion Hubs (XHubs) are connected to the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module, “Xhub” is displayed in the Requested State fields under Expansion Port Configuration in the lower half of the **Local Switch** tab of the Site Controller Switch window. See Figure 15: CSS Site Controller Switch Window – Expansion Port Configuration Area on page 46.
- The Port Security fields in this area of the **Local Switch** tab display the security settings for the front ports on the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module that are connected to the XHubs.
- You can view Port Security settings for the ports located on a specific XHub device by clicking the tab for that XHub device at the top of the Site Controller Switch window (for example the “XHub1” tab shown in Figure 14: CSS Site Controller Switch Window – Local Switch Tab on page 45).

Figure 15: CSS Site Controller Switch Window – Expansion Port Configuration Area



6.6 Capturing the MAC Address of a Device Connected to a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module

When and where to use: Follow these steps to capture the MAC address of a device connected to a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module. Before enabling MAC Port Lockdown on the Ethernet ports on the internal switch of a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module, the MAC address of the device to be locked must be learned by the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module. The GCP 8000 Site Controller will not learn any MAC addresses after configuring the port security.

IMPORTANT: MAC Port Lockdown cannot be applied to the switch ports connected to redundant routers at ASTRO® 25 Repeater Sites with GTR 8000 Base Radios.

Procedure:

1 Connect one or more devices to their Ethernet ports on the internal switch or Expansion Hubs (XHubs) of the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module.

2 Power up all devices. Wait for one minute until the device establishes a connection with the port on the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module.

The MAC address of the device is learned by the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module port.

3 Enable MAC Port Lockdown on all the ports for GCP 8000 Site Controllers or GPB 8000 Reference Distribution Modules.

See Enabling/Disabling 802.1x and MAC Port Lockdown for GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with CSS on page 47.

6.7

Enabling/Disabling 802.1x and MAC Port Lockdown for GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with CSS

Prerequisites:

- This procedure assumes that RADIUS authentication has been configured for the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module. See the *Authentication Services* manual.
- Configuration parameters selected using the Configuration/Service Software (CSS) may be overwritten by the central configuration tool, especially if they do not pass the compliance checks by that tool. For information on configuration compliance for your system, contact your system administrator.
- Ports connected to redundant routers at ASTRO® 25 Repeater Sites with GTR 8000 Base Radios and IP Simulcast remote subsites cannot be locked.
- If you are enabling MAC Port Lockdown, ensure that the MAC address of the device has been captured using the procedure provided in Capturing the MAC Address of a Device Connected to a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module on page 46.

CAUTION: When implementing Ethernet port security with CSS, ensure that all externally accessible switch ports (including ports on attached XHub devices) have Port Security configured to Locked, 802.1x or have Requested State configured to Inactive.

When and where to use: Follow these steps to enable/disable 802.1x and MAC Port Lockdown on a port-by-port basis through CSS. The procedure uses the **Port Security** field on the Site Controller Switch window. You can use this procedure when you need port-by-port configuration capability, for greater flexibility than the centralized VoyenceControl/Unified Network Configurator tools provide for enabling/disabling 802.1x and MAC Port Lockdown at GCP 8000 Site Controller or GPB 8000 Reference Distribution Module sites.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.
In the CSS application, the window name is **Site Controller Switch** for GCP 8000 Site Controller, and **Switch Configuration** for GPB 8000 Reference Distribution Module.

Procedure:

1. To access the Site Controller Switch window in CSS, follow the steps in Viewing Ethernet Port Security for the GCP 8000 Site Controller and GPB 8000 Reference Distribution Module with CSS on page 45.
2. To enable or disable Ethernet Port Security on a specific port, click the cell for that port in the **Port Security** column.

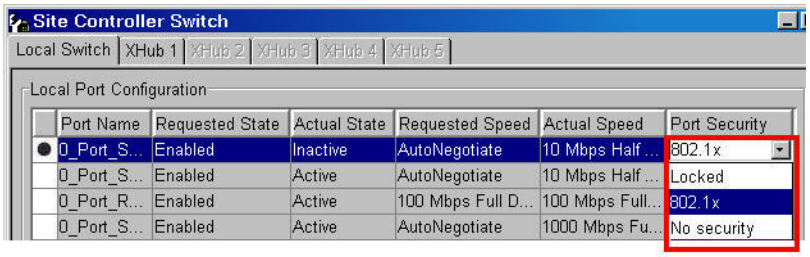
   NOTICE: Port Security settings for Ports 1, 4, 6 and 13 through 17 are read-only, set to No Security, and cannot be changed.

   The drop-down menu displays (this menu is highlighted in Figure 16: CSS Site Controller Switch Window – Port Security Menu on page 48).
3. Select one of the following options from the drop-down menu:

If…	Then…
You want to enable MAC Port Lockdown (so that this portdoes not learn any more MAC addresses),	click **Locked** in the drop-down menu.

If…	Then…
You want to enable 802.1x (so that this port provides authenticated access to the network),	click **802.1x** in the drop-down menu.
You want to disable both MAC Port Lockdown and 802.1x for this port,	click **No Security** in the drop-down menu.

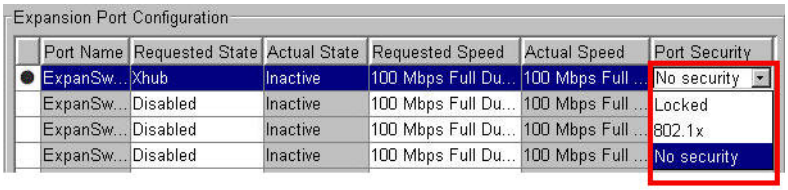
Figure 16: CSS Site Controller Switch Window – Port Security Menu



Your selection appears in the Port Security column for the port. This selection takes effect when you write the configuration to this GCP 8000 Site Controller or GPB 8000 Reference Distribution Module device.

4 If Expansion Hubs (XHubs) are connected to that GCP 8000 Site Controller or GPB 8000 Reference Distribution Module, then “Xhub” will be displayed in the Requested State fields under Expansion Port Configuration in the lower half of the Local Switch tab of the Site Controller Switch window. To set the Port Security for the front ports on the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module that are connected to the XHubs, use the **Port Security** fields under Expansion Port Configuration in the lower half of the Local Switch tab.

Figure 17: CSS Site Controller Switch Window – Expansion Port Security Menu



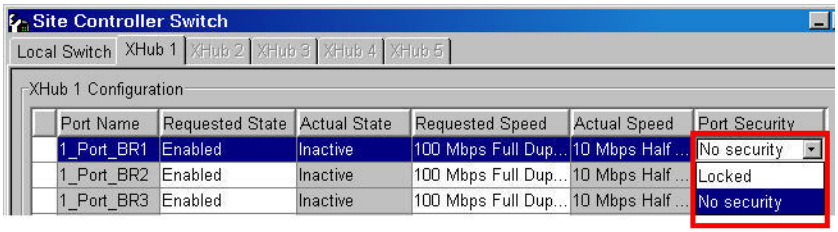
5 To set the port security for the ports located on a specific XHub device, perform the following steps:

a Click the tab for that XHub device at the top of the Site Controller Switch window (for example, the “XHub1” tab shown in Figure 18: CSS Site Controller Switch Window – XHub Port Security Menu on page 48).

b Click the cell in the **Port Security** column for a port on the XHub.

c To enable or disable MAC Port Lockdown for this port, use the drop-down menu.

Figure 18: CSS Site Controller Switch Window – XHub Port Security Menu



NOTICE: 802.1x configuration is not available for ports on an XHub device.

Your selection appears in the Port Security column for the port.

6 Create an archive file using the following steps:

a Click **Save** or **Save As** from the **File** menu.

b Enter any desired information about the file, such as your name in the **Changed By** field. Click **OK**.

c Enter a name for the file in the **File name** field, then specify a directory location in which to save the file. Click **Save**.

7 Write the configuration data to the device. Select **File** → **Write Configuration to Device** from the menu bar.

CSS writes the configuration data to the device. A confirmation window appears.

8 Click **OK** to close the window.

IMPORTANT: Some parameters are classified as Reset parameters, as indicated by an [R] after the parameter name in the configuration screens. If a configuration file in which one or more of this type of parameter value has been modified, a confirmation window will appear to notify you that a reset will be initiated after the configuration data has been written to the device.

- If you click **OK**, the device automatically resets after the device receives and stores the new configuration data.
- If you click **Cancel**, CSS will write the parameters to the device but the parameters will not take effect until a reset occurs.

6.8 Enabling/Disabling MAC Port Lockdown on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with Site Wizards

To perform MAC Port Lockdown on the Ethernet ports on the internal switch of a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module in an ASTRO® 25 system, you can use the appropriate Site Wizard in the Unified Network Configurator (UNC). On the Site Configuration screen, select one of the following options for “MAC Port Lockdown State”:

- Locked
- Unlocked

Before performing this procedure, ensure that the MAC address of the device has been captured using the procedure provided in Capturing the MAC Address of a Device Connected to a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module on page 46.

NOTICE: If there are redundant GCP 8000 Site Controllers or GPB 8000 Reference Distribution Modules at the site, this locks the Ethernet ports on both of the site controllers.
If there are XHubs connected to the site controller, this locks all of the Ethernet ports on the XHub as well.

CAUTION: All unused externally accessible switch ports (including ports on attached XHub devices) should be configured to be disabled before enabling Ethernet port security on the remaining ports. Refer to *CSS Online Help* for details on how to disable switch ports.

The Site Wizard does not lock the ports that are connected to routers. To lock these ports, see Enabling/Disabling 802.1x and MAC Port Lockdown for GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with CSS on page 47.

Information about using Site Wizards in UNC is available in the *Unified Network Configurator* manual.

6.9 Validating MAC Port Lockdown on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module

Process:

1. Identify two ports on the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with port security set to the “Locked” state and connected to two devices.
2. Swap the cables between the two ports.
3. Verify that the devices can no longer communicate. See Table 3: Methods for Verifying MAC Port Lockdown on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with Ethernet Cables Swapped on page 50.
4. Connect the devices back to the ports on which they were originally connected.
5. Verify that the devices can now communicate using LEDs, Configuration/Service Software (CSS), and Unified Event Manager (UEM). For instructions, refer to the documentation listed in Table 3: Methods for Verifying MAC Port Lockdown on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with Ethernet Cables Swapped on page 50.

6.9.1 Methods for Verifying MAC Port Lockdown on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module

To verify MAC Port Lockdown on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module, start by swapping cables between two GCP 8000 Site Controller or GPB 8000 Reference Distribution Module Ethernet ports where MAC Port Lockdown was implemented. Then, perform the actions in the following table.

Table 3: Methods for Verifying MAC Port Lockdown on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with Ethernet Cables Swapped

MAC Port Lockdown Verification Method	For additional information, see:
Check the Status and Alarm LEDs on the devices that are now connected to the wrong GCP 8000 Site Controller or GPB 8000 Reference Distribution Module ports. The LEDs should indicate the device is NOT online.	ASTRO® 25 system manuals for the devices being tested
1 Connect to the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module Ethernet service port through Configuration/Service Software (CSS). 2 Select **Service** → **Status Report Screen** in CSS. Alarms and changes in status display. 3 Additionally, log files associated with the device are managed from this location.	*CSS Online Help*

Table continued…

MAC Port Lockdown Verification Method	For additional information, see:
1 Access the Unified Event Manager (UEM) fault management tool. **2** Check for faults on devices at the remote site with this GCP 8000 Site Controller or GPB 8000 Reference Distribution Module, using the UEM Topology Maps or Active Alarms Window. **NOTICE:** If the site gateway or site switch is currently connected to the wrong port on the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module, check for a fault on the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module. Otherwise, check for faults on the devices that are currently connected to the wrong port on the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module.	*Unified Event Manager* manual

6.10

Unlocking/Locking the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module Ethernet Port When Replacing a Site Gateway

Prerequisites: This procedure starts by disabling 802.1x, with the assumption that the network is not available due to a site gateway failure.

When and where to use: Follow these steps to update the Ethernet port security configuration for the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module when replacing a site gateway.

Process:

1. Disable 802.1x on the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module Ethernet service port. See Disabling 802.1x on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module Ethernet Port with the Serial Port on page 85.
2. Disconnect the service laptop from the serial port.
3. Connect the service laptop to the Ethernet front panel service port on the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module.
4. Read the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module configuration in CSS. For instructions, refer to *CSS Online Help*.
5. Disconnect the faulty site gateway from the GCP 8000 site gateway or GPB 8000 Reference Distribution Module port.
6. Connect the replacement site gateway to the GCP 8000 site gateway or GPB 8000 Reference Distribution Module port.
7. Access the Site Controller Switch window in CSS. See Viewing Ethernet Port Security for the GCP 8000 Site Controller and GPB 8000 Reference Distribution Module with CSS on page 45.
8. Change the port security setting on the router port to "No Security". See Enabling/Disabling 802.1x and MAC Port Lockdown for GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with CSS on page 47.
9. Write the configuration to the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module from CSS. For instructions, refer to *CSS Online Help*.

10 Ping the GCP 8000 Site Controller from the new site gateway and verify that the ping is successful.

11 In the Site Controller Switch window on CSS, change the port security setting on the router port to "Locked". See Enabling/Disabling 802.1x and MAC Port Lockdown for GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with CSS on page 47.

12 Write the configuration to the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module from CSS.

13 In the Site Controller Switch window on CSS, change the port security setting on the service port to "802.1x". See Enabling/Disabling 802.1x and MAC Port Lockdown for GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with CSS on page 47.

14 Write the configuration to the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module from CSS.

6.11 MAC Port Lockdown Procedures for HP Switches – Overview

General procedures:

- HP Switches – Accessing the Console Interface on page 54
- Logging on to an HP Switch with Cut-Through on page 56
- Logging out of an HP Switch with Cut-Through on page 57
- Displaying HP Switch Port Status – Overview on page 57

See MAC Port Lockdown Operation on page 43 for additional general information that may be useful when performing the following MAC Port Lockdown procedures on switches. For example, you can use the instructions in the chapter each time the following procedures require use of the VoyenceControl component of Motorola's Unified Network Configurator.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

MAC Port Lockdown procedures for HP switches:

- Performing MAC Port Lockdown on HP Switches on page 52
- Disabling MAC Port Lockdown with Cut-Through in VoyenceControl on page 69
- Disabling MAC Port Lockdown with an HP Switch Service Port on page 71
- Changing the Address Limit on a Previously Configured HP Switch Port on page 71

NOTICE: Relocking and re-enabling a port is required if the port was disabled due to an access attempt by a device with an unauthorized MAC address. You can view the MAC address of an unauthorized device on an HP switch by entering the following at the command line at the switch. The following command displays the Port, MAC Address, and Date/Time:

```
show port-security intrusion-log
```

HP switch "port-security" commands are only used for MAC Port Lockdown functions, not 802.1x functions.

6.12 Performing MAC Port Lockdown on HP Switches

Prerequisites: Before performing this procedure, consider the following:

- How many devices are connected at each site?
- Are the devices plugged in at the site correct?

- Is there connectivity to the site?
- See MAC Port Lockdown Description on page 23 for a list of Ethernet switches in an ASTRO® 25 system.

When and where to use: The MAC Port Lockdown feature should be applied to all Ethernet switches in the system. The following process provides an overview of the procedures that are required to perform MAC Port Lockdown on all Ethernet switches in the system.

Process:

1. Disable all unused ports. See:
   - Enabling/Disabling Ports on HP Switches with Local Access on page 86
   - Enabling/Disabling Ports on HP Switches with VoyenceControl on page 87

   NOTICE: If faults appear in the Unified Event Manager for 802.1x service ports that have no device connected to them, these faults can be removed if desired, by disabling these service ports when they are not being used by a service technician.
2. In order to determine whether each used port has previously been configured for port security, see Displaying Port Security for HP Switches with a Saved Command on page 57.
3. Perform the following, if needed, depending whether the port was previously configured for MAC Port Lockdown:

If…	Then…
The port has been previously configured for MAC Port Lockdown and has learned a MAC address,	see Disabling MAC Port Lockdown with Cut-Through in VoyenceControl on page 69.
The port has not been previously configured for MAC Port Lockdown,	see step 4.

4. Perform the following, depending which port you are locking:

If…	Then…
The switch port is connected to a router in a redundant configuration,	see Locking MAC Ports on HP Switches in Redundant Site-Link Configurations on page 62.

If…	Then…
NOTICE: This includes the master site core, exit, and gateway routers. **Additionally, you can view the HP switch configurations for your ASTRO® 25 system to determine whether any HP switch ports connect to the following types of routers in redundant configuration:** • **IP Simulcast prime site gateways (primary routers and remote site access routers)** • **IP Simulcast remote site gateways** • **Simulcast prime site gateways** • **Simulcast remote site gateways** • **Geographically redundant prime site gateways**	
The switch port is used but is not connected to a router in a redundant configuration,	perform the following steps: **a** Before locking the port, follow the steps in: Determining the Number of MAC Addresses Learned by a Port on page 59. **b** Lock each used port, using one of the following procedures: • Locking HP Switch Ports with a VoyenceControl Template on page 60 • Locking HP Switch Ports on page 61 **NOTICE:** You need to lock each port or ports that have a different number of MAC addresses, as indicated when you performed the procedure in: Determining the Number of MAC Addresses Learned by a Port on page 59.

5 Verify that the locked ports are enabled. See Validating MAC Port Lockdown on HP Switches on page 68.

6.13 HP Switches – Accessing the Console Interface

HP switches feature a menu interface that is used to do the following:

- Monitor the switch and port status and observe network activity counters
- View the switch configuration

- Read the event log and access diagnostic tools to help in troubleshooting
- Download new software to the switch
- Add passwords and other security features to control access to the switch from the console and network management stations

The menu interface is accessed using either a direct connection through the console port or through a telnet session.

The HP ProCurve Series switch simultaneously supports one connection of each type at the same time.

6.13.1
Accessing the HP Switch Console with Telnet or SSH

Prerequisites:
The switch must be configured with an IP address and subnet mask. Contact your administrator for this information.

Procedure:

1. To find or set the service laptop IP address, click **Start** → **Settings** → **Control Panel**. Double-click the **Network** icon and select the **Protocols** tab.
2. Verify that the switch is reachable by pinging its IP address.
3. Start the Telnet or SSH program and connect to the switch's IP address.

   The copyright page appears. A prompt appears to press any key to continue.
4. Press any key.

   The switch console Command Line Interface (CLI) appears.
5. If you are prompted for a password, type it and press ENTER.

   NOTICE: If RADIUS is enabled on the switch, you must log on with a RADIUS client user account that is set up in the Network Policy Server (NPS) RADIUS server on the domain controllers. An administrator RADIUS user group and a read-only RADIUS user group are set up by Motorola Solutions in the NPS, with a “serviceuser” account is set up in the administrator group by Motorola Solutions. For more information, see the *Authentication Services* manual.
   When you log on with a local account, entering the Manager password provides you with manager-level access to the switch. Entering the Operator password provides you with operator-level access to the switch. If you are not prompted for a password, it means that it has not been configured.

   The command line interface prompt appears.

6.13.2
Establishing Direct Console Access to the HP Switch

Prerequisites: Before performing this procedure, obtain the following:

- Service laptop with a terminal emulator such as Microsoft HyperTerminal, or with PuTTY installed
- Serial cable (female DB9-to-female DB9)
- Ethernet cable
- Current IP address of the switch

Procedure:

1. Connect a service laptop or terminal to the switch console port using the console cable that came with the switch.

   NOTICE: If the PC or the terminal has a 25-pin serial connector, first attach a 9-pin to 25-pin straight-through adapter to the PC end of the console cable.

2. Turn on the service laptop or terminal's power.

   NOTICE: If using a service laptop, start the terminal emulator program, such as Microsoft HyperTerminal.

3. Configure the terminal or terminal emulator as follows:
   - Baud rate should be 9600
   - 8 data bits, no parity, no flow control
   - 1 stop bit
   - No parity
   - No flow control
   - Functional, arrow, and CTRL keys act as terminal keys
4. Press ENTER until you see the copyright message and the prompt to press any key to continue.
5. Press any key.

   The switch console Command Line Interface (CLI) appears. If you are prompted for a password, type it and press ENTER.

6. If you are prompted for a password, type it and press ENTER.

   NOTICE: Entering the local Manager password provides you with manager-level access to the switch. Entering the local Operator password provides you with operator-level access to the switch. If you are not prompted for a password, it means that it has not been configured.

6.14 Logging on to an HP Switch with Cut-Through

Prerequisites: Before performing this procedure, the devices in the procedures need to be discovered in VoyenceControl and their configurations need to be recently pulled.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

When and where to use: Follow these steps to access the command line for a switch, using the Cut-Through feature in VoyenceControl.

Procedure:

1. Log into VoyenceControl.

   The VoyenceControl main window appears.

2. In the navigation pane on the left side of the window, double-click **Astro 25 Radio Network**.

   The selected network tree expands to display the Devices node.

3. In the navigation pane on the left side of the window, double-click **Devices**.

   The Devices View appears. The list of devices and associated properties is displayed in the pane on the right side of the screen.

4 Right-click the desired switch in the Devices View pane on the right side of the screen, and select **Cut-Through** → **In-band** from the context menu.

   The command line session window for the switch appears.

5 Click inside the command line session window and press ENTER.

   The switch command line prompt appears and you are logged on.

6.15 Logging out of an HP Switch with Cut-Through

When and where to use: Follow these steps to log out of an HP switch using the Cut-Through feature of VoyenceControl.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

Procedure:

1 In the VoyenceControl command line window, type `logout` and press ENTER.

   An option to log out appears.

2 Type `y` to log out.

   An option to save the current configuration may appear (for example, if you made configuration changes but did not use the “write memory” command). To save the current configuration locally, type `y`.

3 When a message appears stating that the connection has been lost, close the command line window.

   The VoyenceControl window re-appears.

6.16 Displaying HP Switch Port Status – Overview

There are several ways to display port status to prepare for or validate port configuration procedures.

- Follow the steps in Displaying Port Security for HP Switches with a Saved Command on page 57.
- Use the `show port-security` command, as indicated in Determining the Number of MAC Addresses Learned by a Port on page 59.
- There are other commands that display useful port status information, including `show interfaces brief` ***`<port(s)>`***, which can be used to determine if a port is enabled/disabled and whether the port is up/down.

6.17 Displaying Port Security for HP Switches with a Saved Command

When and where to use: Follow these steps to determine the number of MAC addresses the switch has detected on a port or ports, and also to display the current state of the ports (locked or unlocked).

NOTICE: For information on setup and login, and additional ways to use VoyenceControl, see the *Unified Network Configurator* manual.
The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

Procedure:

1. Log into VoyenceControl.

   The VoyenceControl main window appears.

2. In the navigation pane on the left side of the window, double-click **Astro 25 Radio Network**.

   The selected network tree expands to display the Devices node.

3. In the navigation pane on the left side of the window, double-click **Devices**.

   The Devices View appears. The list of devices and associated properties are displayed in the pane on the right side of the screen.

4. Right-click the desired switch in the Devices View pane on the right side of the screen, and select **Saved Commands** from the context menu.

   The Select Item dialog box displays.

5. Click the folder icon at the top of the dialog box, to the right of the **Look in** field. Continue to click this icon until the **System** folder displays in the list of folders on the Select Item dialog box.
6. In the list of folders on the Select Item dialog box, double-click the **System** folder, then double-click the **Motorola** folder, and then double-click the **HP** folder.

   A list of saved commands displays on the Select Item dialog box.

7. Double-click the saved command named **Show Port(s) Security**.

   The Template Variable Substitution window displays.

8. Type the port number(s) for which you want to view security information, and then click **OK**.

   Step example:

   - For port number 3, type `3`
   - For port numbers a3, a5, a6, and a7, type `a3, a5-a7`

   You can enter up to 20 characters in the **Ports** field. If you reach the maximum of 20 characters (for example, when entering multiple non-contiguous port numbers), then you will need to execute the command again for the remaining port numbers.

   A progress window appears. After approximately 30 seconds, the Results dialog box appears. If the command is executed successfully, the switch appears in the **Successful Results** list.

9. Click the device in the **Successful Results** list.

   The results appear in the **Results** field.

   - The port is locked if `Static` displays after the colon (:) on the Learn Mode line of the results.
   - `(Continuous)` displayed within parenthesis indicates the default mode, and not the current mode.

6.18

Determining the Number of MAC Addresses Learned by a Port

Prerequisites: Before performing this procedure, obtain the IP addresses for the virtual server host and the following virtual machines:

- Backup and Recovery Server virtual machine
- Centralized Event Logging Server virtual machine
- Firewall Management Server virtual machine (if present in this zone)
- Domain Controller/Authentication Server virtual machine (if present in this zone)

Contact your system administrator for the information.

When and where to use: Follow these steps before enabling port security (MAC Port Lockdown), if you do not already know the number of MAC addresses learned by a port. This procedure provides the number of MAC addresses learned, which you need to include in the command that enables port security.

Procedure:

1. Perform one of the following procedures to log on to the switch and open a command line session:
   - Accessing the HP Switch Console with Telnet or SSH on page 55
   - Establishing Direct Console Access to the HP Switch on page 55
   - Logging on to an HP Switch with Cut-Through on page 56

   A command line window appears.
2. Type `config`
3. Type the following command to learn the MAC addresses on the port:

   `port-security <port> learn-mode static address-limit 31`

   NOTICE: The switch port does not learn the MAC address(es) of the connected device dynamically. After entering the port-security command, you may have to ping the device for the switch to learn its MAC address(es).
   Note that the switch port connected to the virtual server needs to learn the MAC addresses of all the virtual machines hosted on that server, as well as the MAC address for the virtual server host. Ping all those IP addresses, as indicated in the Prerequisites above this procedure.
4. Type the following command to determine the number of MAC addresses:

   `sh port-security <port>`

   In the command output, the MAC addresses associated with the port are displayed.
5. From the command output, count the MAC addresses associated with the port.

   This count is the number of MAC address(es) learned/reported by that port.

   IMPORTANT: If the reported number of MAC addresses is 32 or higher, the port cannot have port security enabled. See Disabling MAC Port Lockdown with Cut-Through in VoyenceControl on page 69 to remove port security on a port that reports more than 31 MAC addresses. It is recommended that your system administrator be informed about any ports which cannot have port security enabled.
6. To learn the MAC address(es) for another port, repeat this procedure starting at step 2.
7. When the ports have finished learning the MAC addresses:

If…	Then…
If you want to use a template in VoyenceControl to enable port security, **NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.**	log out and close the command line window.
If you want to enable port security for this device using command lines,	proceed to Locking HP Switch Ports on page 61.

8 Log out and close the command line window.

The VoyenceControl Devices view displays, if you are using VoyenceControl to access the switch. Otherwise you are returned to the application you used to establish the connection.

6.19

Locking HP Switch Ports with a VoyenceControl Template

To lock the MAC address (enable port security) for one port, or multiple ports that report the same number of MAC addresses, on an HP switch that is connected and has its configuration maintained in VoyenceControl, use the process in Using a Motorola Solutions Template in VoyenceControl on page 87 and the information provided in the following table.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

IMPORTANT: You can enter multiple ports in the ports field only if they reported/learned the same number of MAC addresses. Repeat the template procedure individually for every port that reported/learned a different number of MAC addresses. If you are enabling port security on a switch port that connects to routers in a redundant configuration, do not use this template. Instead, use Locking MAC Ports on HP Switches in Redundant Site-Link Configurations on page 62.

Table 4: Template Information to Lock HP Switch Ports

Task You Are Performing	Subfolder Where Template is Located	Name of the Template	Variable Fields That Require Input
Locking the MAC address for one port, or multiple ports that report the same number of MAC addresses, on an HP switch	(under **System → Motorola**): **HP**	Lock Port(s) To Current MAC	• Ports to be locked (do not include ports for redundant routers) • Number of MAC addresses reported/learned (can be a number from 1 to 31)

Examples of values for the Ports field:

- For port number 3, type 3
- For port numbers a3, a5, a6, and a7, type `a3, a5-a7`

You can enter up to a maximum of 20 characters in the **Ports** field. If you reach the maximum of 20 characters (for example, when entering multiple non-contiguous port numbers), then you will need to perform the procedure again for the remaining port numbers.

6.20 Locking HP Switch Ports

Prerequisites:
Obtain the IP addresses for the virtual server host and the following virtual machines:

- Backup and Recovery Server virtual machine
- Centralized Event Logging Server virtual machine
- Firewall Management Server virtual machine (if present in this zone)
- Domain Controller/Authentication Server virtual machine (if present in this zone)

Also, perform the following:

- Determine whether the port has previously been configured for port security. Follow the steps in Displaying Port Security for HP Switches with a Saved Command on page 57.
- Determine the number of learned MAC addresses for the port. Follow the steps in Determining the Number of MAC Addresses Learned by a Port on page 59.
- If a port is previously configured for port security and has learned a MAC address, follow the steps in Disabling MAC Port Lockdown with Cut-Through in VoyenceControl on page 69 to disable port security.

When and where to use: Perform these steps to lock the MAC address (enable port security) for one port, or multiple ports that report the same number of MAC addresses, on an HP switch.

IMPORTANT: If you are enabling port security on a switch port that connects to routers in a redundant configuration, do not use the following procedure. Instead, follow the steps in Locking MAC Ports on HP Switches in Redundant Site-Link Configurations on page 62.

Procedure:

1. Perform one of the following procedures to log on to the switch and open a command line session:
   - Accessing the HP Switch Console with Telnet or SSH on page 55
   - Establishing Direct Console Access to the HP Switch on page 55
   - Logging on to an HP Switch with Cut-Through on page 56

   A command line window appears.
2. Type `config`.
3. Type the following command to set port security (enable MAC Port Lockdown) for ports other than redundant router ports:

   `port-security` ***`<port(s)>`*** `learn-mode static address-limit` ***`<numberMacAllowed>`*** `action send-Disable`
   where ***`<numberMacAllowed>`*** specifies the number of MAC addresses reported for this port before you started this procedure.

   For information regarding the ***`<port(s)>`*** variable, see Locking HP Switch Ports with a VoyenceControl Template on page 60.

NOTICE: The switch does not learn the MAC address(es) of the connected device dynamically. You may have to ping the device for the switch to learn its MAC address(es).
The switch port connected to the virtual server needs to learn the MAC addresses of all the virtual machines hosted on that server, as well as the MAC address for the virtual server host. Ping all those IP addresses, as indicated in the Prerequisites above this procedure.

Port security is enabled on port(s) locking to the learned MAC address(es), and an alarm message is sent when a violation occurs and the port is disabled (detection takes about 10 seconds).

4. Type the following command to make the changes permanent:

   ```
   write memory
   ```

5. Type the following command to determine the MAC address(es) that the switch has detected and locked to, for a particular port or range of ports:

   ```
   sh port-security <port(s)>
   ```

6. Type the following command to check the status of all the ports on the switch:

   ```
   show interfaces brief
   ```

   IMPORTANT: Ensure that all the required ports are enabled and the status is Up. Also, ensure that all the unwanted ports are disabled.

7. To save the configuration on your PC type the following:

   ```
   copy startup-config tftp <ip address><file name>
   ```

   where ***<ip address>*** is the IP address of your computer, where the configuration is to be saved, ***<file name>*** is the name the saved file will have.

   NOTICE: See the *System LAN Switches* manual for local procedures using SCP when connecting through SSH.

   A configuration file is saved on your computer.

8. Log out and close the command line window.

   If you are validating a change to the configuration of the port, proceed to step 9 in order to pull the configuration change into VoyenceControl.

   NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

   The VoyenceControl Devices view displays, if the connection to the switch wasn't through a telnet/SSH application or a direct console connection.

9. Right-click the desired switch in the Devices View pane on the right side of the screen, and select **Pull** → **Pull Config** from the context menu.

   The switch configuration is uploaded to the VoyenceControl database.

6.21 Locking MAC Ports on HP Switches in Redundant Site-Link Configurations

The following procedure is used to apply a MAC port lock on HP switches in redundant site-link configurations. This procedure is executed manually using direct access through the console ports.

Guide to Locking MAC Ports on HP Switches in Redundant Site-Link Configurations on page 65 outlines in a table format the steps listed in this procedure. Use the guide as a help in understanding the actions required for each device.

This operation is performed at a site and takes about 10 minutes per site. A site goes down momentarily when the routers are rebooted.

Redundant sites include the following site types:

- Repeater site
- Simulcast prime site
- Simulcast subsite
- Console site
- Conventional Subsystem Architecture (CSSA) sites:
  - Base Radio (BR) site
  - Conduit hub site
  - Hub site

The command lines used in the MNR router models S2500, S6000, and Transport Gateway (GGM8000) are identical.

The command lines used in the HP switches are identical in all models including HP2620-24, HP2620-48, HP3500-24, HP3800-48.

NOTICE: This procedure assumes the following configuration:

- Port 1 of router 1 connects to port 1 of HP switch 1.
- Port 1 of router 2 connects to port 1 of HP switch 2.

For some sites, for example, simulcast prime sites, the configuration can be different.

Prerequisites:
Ensure that the redundant site links are up and operational.

Ensure that the service personnel is at a remote site to execute the procedure.

Procedure:

1. Log on to the following devices through the console ports using the appropriate user name and password.
   - Router 1
   - Router 2
   - Switch 1
   - Switch 2
2. In router 1, verify that the Virtual Router ID (VRID) is 1. At the command line, enter: `sh –vrrp vrid`
3. In router 2, verify that the VRID is 2. At the command line, enter: `sh –vrrp vrid`
4. In switch 1, at the command line, enter: `config`
5. In switch 2, at the command line, enter: `config`
6. In switch 1, enable port-security learning mode on port 1 that connects to router 1. At the command line, enter: `port-security 1 learn-mode static address-limit 31`
7. In switch 2, enable port-security learning mode on port 1 that connects to router 2. At the command line, enter: `port-security 1 learn-mode static address-limit 31`

8 In switch 1, verify that port 1 has learned the VRRP MAC port address of router 1. At the command line, enter: `show port-security 1`

The VRRP MAC port address of router 1 is `00005e-000101`.

9 In switch 2, verify that port 1 has learned the VRRP MAC port address of router 2. At the command line, enter: `show port-security 1`

The VRRP MAC port address of router 1 is `00005e-000102`.

10 In router 2, disable VRID 1. At the command line, enter: `setd !1 –vrrp control = disable 1`

11 In router 1, disable VRID 1. At the command line, enter: `setd !1 –vrrp control = disable 1`

12 In switch 1, verify that port 1 has learned the physical MAC port address of router 1. At the command line, enter: `show port-security 1`

Two MAC port addresses appear:

- VRRP MAC port address of router 1
- Physical MAC port address of router 1

13 In router 1, enable VRID 1. At the command line, enter: `setd !1 –vrrp control = enable 1`

14 In router 2, enable VRID 1. At the command line, enter: `setd !1 –vrrp control = enable 1`

15 In router 1, disable VRID 2. At the command line, enter: `setd !1 –vrrp control = disable 2`

16 In router 2, disable VRID 2. At the command line, enter: `setd !1 –vrrp control = disable 2`

The WAN link on router 2 goes down.

17 In router 1, enable VRID 2. At the command line, enter: `setd !1 –vrrp control = enable 2`

18 In switch 2, verify that port 1 has learned the physical MAC port address of router 2. At the command line, enter: `show port-security 1`

Two MAC port addresses appear:

- VRRP MAC port address of router 2
- Physical MAC port address of router 2

19 Reboot router 2. At the command line, enter: `reboot`

The reboot takes about two minutes.

20 In switch 1, verify that port 1 has learned the VRRP MAC port address of router 2. At the command line, enter: `show port-security 1`

Three MAC port addresses appear:

- VRRP MAC port address of router 1
- VRRP MAC port address of router 2
- Physical MAC port address of router 1

21 Reboot router 1. At the command line, enter: `reboot`

The reboot takes about two minutes.

22 In switch 2, verify that port 1 has learned the VRRP MAC port of router 1. At the command line, enter: `show port-security 1`

Three MAC port addresses appear:

- VRRP MAC port address of router 1
- VRRP MAC port address of router 2
- Physical MAC port address of router 2

23 In switch 1, apply MAC port lock on port 1. At the command line, enter: `port-security 1 learn-mode static address-limit 31 action send-Disable`

24 In switch 2, apply MAC port lock on port 1. At the command line, enter: `port-security 1 learn-mode static address-limit 31 action send-Disable`

25 In switch 1, save the configuration. At the command line: `write mem`

26 In switch 2, save the configuration. At the command line: `write mem`

6.22

Guide to Locking MAC Ports on HP Switches in Redundant Site-Link Configurations

This topic outlines in a table format the sequence of steps performed to lock MAC port switches in redundant site-link configurations. The table covers the same steps as the procedure for locking MAC port switches and is provided to help you understand the actions required for each device.

For prerequisites, additional information, and the step-by-step procedure, see Locking MAC Ports on HP Switches in Redundant Site-Link Configurations on page 62.

Table 5: Guide to Locking MAC Ports on HP Switches in Redundant Site-Link Configurations

Step	Router 1	Switch 1	Router 2	Switch 2
1	Log on to router 1 through the console ports using the appropriate user name and password.	Log on to switch 1 through the console ports using the appropriate user name and password.	Log on to router 2 through the console ports using the appropriate user name and password.	Log on to switch 2 through the console ports using the appropriate user name and password.
2	Verify that the Virtual Router ID (VRID) is 1. At the command line, enter: `sh –vrrp vrid`	At the command line, enter: `config`	Verify that the VRID is 2. At the command line, enter: `sh –vrrp vrid`	At the command line, enter: `config`
3		Enable port-security learning mode on port 1 that connects to router 1. At the command line, enter: `port-security 1`		Enable port-security learning mode on port 1 that connects to router 2. At the command line, enter: `port-security 1`

Table continued…

Step	Router 1	Switch 1	Router 2	Switch 2
		`learn-mode static address-limit 31`		`learn-mode static address-limit 31`
4		Verify that port 1 has learned the VRRP MAC port address of router 1. At the command line, enter: `show port-security 1` The VRRP MAC port address of router 1 is `00005e-000101`.		Verify that port 1 has learned the VRRP MAC port address of router 2. At the command line, enter: `show port-security 1` The VRRP MAC port address of router 1 is `00005e-000102`.
5			Disable VRID 1. At the command line, enter: `setd !1 –vrrp control = disable 1`	
6	Disable VRID 1. At the command line, enter: `setd !1 –vrrp control = disable 1`	Verify that port 1 has learned the physical MAC port address of router 1. At the command line, enter: `show port-security 1` Two MAC port addresses appear: • VRRP MAC port address of router 1 • Physical MAC port address of router 1		
7	Enable VRID 1. At the command line, enter: `setd !1 –vrrp control = enable 1`		Enable VRID 1. At the command line, enter: `setd !1 –vrrp control = enable 1`	
8	Disable VRID 2. At the command line, enter: `setd !1 –vrrp control = disable 2`		Disable VRID 2. At the command line, enter: `setd !1 –vrrp control = disable 2` The WAN link on router 2 goes down.	

Table continued...

Step	Router 1	Switch 1	Router 2	Switch 2
9	Enable VRID 2. At the command line, enter: `setd !1 –vrrp control = enable 2`			
10				Verify that port 1 has learned the physical MAC port address of router 2. At the command line, enter: `show port-security 1` Two MAC port addresses appear: • VRRP MAC port address of router 2 • Physical MAC port address of router 2
11			Reboot router 2. At the command line, enter: `reboot` The reboot takes about two minutes.	
12		Verify that port 1 has learned the VRRP MAC port address of router 2. At the command line, enter: `show port-security 1` Three MAC port addresses appear: • VRRP MAC port address of router 1 • VRRP MAC port address of router 2 • Physical MAC port address of router 1		
13	Reboot router 1. At the command line, enter: `reboot`			

Table continued…

Step	Router 1	Switch 1	Router 2	Switch 2
	The reboot takes about two minutes.			
14				Verify that port 1 has learned the VRRP MAC port of router 1. At the command line, enter: `show port-security 1` Three MAC port addresses appear: • VRRP MAC port address of router 1 • VRRP MAC port address of router 2 • Physical MAC port address of router 2
15		Apply MAC port lock on port 1. At the command line, enter: `port-security 1 learn-mode static address-limit 31 action send-Disable`		Apply MAC port lock on port 1. At the command line, enter: `port-security 1 learn-mode static address-limit 31 action send-Disable`
16		Save the configuration. At the command line: `write mem`		Save the configuration. At the command line: `write mem`

6.23

Validating MAC Port Lockdown on HP Switches

When and where to use: Follow these steps to validate the port security configuration.

NOTICE: The results of both step 2 and step 3 should be viewed in order to determine if port security has been set up properly.

Procedure:

1. Perform one of the following procedures to log on to the switch and open a command line session:
   - Accessing the HP Switch Console with Telnet or SSH on page 55
   - Establishing Direct Console Access to the HP Switch on page 55

- Logging on to an HP Switch with Cut-Through on page 56

A command line window appears.

2 At the prompt, type `config`.

3 Type the following command to determine the MAC address(es) that has been detected and locked to by a particular port or range of ports:

`show port-security <port(s)>`

For information regarding the **<port(s)>** variable, see Locking HP Switch Ports with a VoyenceControl Template on page 60.

The list of MAC addresses learned is displayed.

4 Type the following command:

`show interfaces brief <port(s)>`

NOTICE: For all locked ports, the Intrusion Alert flag should be **No**, Enabled flag should be **Yes**, and Status should be **Up**.

5 Repeat step 3 for every port.

6 Type the following command to make the changes permanent:

`write memory`

7 To save the configuration on your PC, type the following:

`copy startup-config tftp <ip address><file name>`

where:
<ip address> is the IP address of your computer, where the configuration is to be saved

<file name> is the name the saved file will have.

NOTICE: Refer to the *System LAN Switches* manual for local procedures using SCP when connecting through SSH.

A configuration file is saved on your computer.

8 Log out and close the command line window when all ports have been verified.

If you are validating a change to the configuration of the port, proceed to step 9 in order to pull the configuration change into VoyenceControl.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

9 Right-click the desired switch in the **Devices View** pane on the right side of the screen, and select **Pull** → **Pull Config** from the context menu.

The switch configuration is uploaded to the VoyenceControl database.

6.24 Disabling MAC Port Lockdown with Cut-Through in VoyenceControl

When and where to use: Follow these steps to disable port security on a port that was previously configured for port security and had learned a MAC address.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

Procedure:

1. Follow the steps in Logging on to an HP Switch with Cut-Through on page 56 to log on to the switch and open a command line session using the Cut-Through method.

   A command line window appears.

2. At the prompt, type `config`.
3. Type the following commands to disable port security on the port:

   a. `no port-security <port(s)>`

   b. `port-security <port(s)>clear-intrusion-flag`

   c. `interface <port(s)> enable`

   d. `write memory`

   For information regarding the **<port(s)>** variable, see Locking HP Switch Ports with a VoyenceControl Template on page 60.

   Port security is disabled on this port.

4. Log out and then close the command line window.
5. Right-click the desired switch in the **Devices View** pane on the right side of the screen, and select **Pull** → **Pull Config** from the context menu.

   The switch configuration is uploaded to the VoyenceControl database.

6.25 Disabling MAC Port Lockdown with a VoyenceControl Template

To disable port security, use the process in Using a Motorola Solutions Template in VoyenceControl on page 87 and the information provided in the following table.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

Table 6: Template Information to Disable Port Security

Task You Are Performing	Subfolder Where Template is Located	Name of the Template	Variable Fields That Require Input
Disabling port security	**System** → **Motorola** → **HP**	Unlock Port(s)	Port number(s) to be unlocked

Examples of values for the Ports field:

- For port number 3, type 3
- For port numbers a3, a5, a6, and a7, type a3, a5-a7

You can enter up to 20 characters in the **Ports** field. If you reach the maximum of 20 characters (for example, when entering multiple non-contiguous port numbers) then you will need to perform the procedure again for the remaining port numbers.

NOTICE: After disabling port security, follow the steps in Displaying Port Security for HP Switches with a Saved Command on page 57 to validate the change.

6.26

Disabling MAC Port Lockdown with an HP Switch Service Port

Prerequisites: This procedure assumes there is local access to the HP switch through its serial service port (console port).

When and where to use: Follow these steps to disable MAC Port Lockdown on an Ethernet port or ports on an HP switch. It is necessary to perform the procedure when network connectivity to VoyenceControl has been disrupted. In order to restore network connectivity, the router connecting to the locked port on the site switch needs to be replaced. The locked port cannot be unlocked through VoyenceControl, so it must be unlocked by gaining access to it through a local service port.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.
To access the HP switch when there is no network connectivity, connect the DB-9 serial port of the service laptop to the console port on the HP switch.

Procedure:

1. Use the service port on the HP switch to log on to the command line for the switch.
2. Type `config`.
3. Type the following commands to disable port security on the port:
   a. `no port-security <port(s)>`
   b. `port-security <port(s)>clear-intrusion-flag`
   c. `interface <port(s)> enable`
   d. `write memory`

   For information regarding the ***<port(s)>*** variable, see Locking HP Switch Ports with a VoyenceControl Template on page 60.

   Port security is disabled on this port.
4. To save the configuration on your PC type the following:

   `copy startup-config tftp <ip address><file name>`

   where:
   <ip address> is the IP address of your computer, where the configuration is to be saved

   <file name> is the name the saved file will have.

   A configuration file is saved on your computer.

6.27

Changing the Address Limit on a Previously Configured HP Switch Port

Procedure:

1. Perform one of the following procedures to log on to the switch and open a command line session:
   - Accessing the HP Switch Console with Telnet or SSH on page 55
   - Establishing Direct Console Access to the HP Switch on page 55
   - Logging on to an HP Switch with Cut-Through on page 56

   A command line window appears.

2 Type `config`.

3 Type the following commands to change the address limit to a desired value:

   a `no port-security` ***<port(s)>***

   b `interface` ***<port(s)>***`enable`

   c `port-security` ***<port(s)>*** `clear-intrusion-flag`

   d `port-security` ***<port(s)>***`learn-mode static address-limit` ***<numberMacAllowed>*** `action send-Disable`

   e `write memory`

   The variable ***<port(s)>*** can be an individual port or a range of ports. For information regarding the variable, see Locking HP Switch Ports with a VoyenceControl Template on page 60.

   The variable ***<numberMacAllowed>*** is the new address limit that can be from 1 to 31 and specifies the number of allowed MAC addresses on port(s).

   The address limit is set to the value specified in ***<numberMacAllowed>***.

4 Validate MAC port lockdown. Follow the steps in Validating MAC Port Lockdown on HP Switches on page 68.

Chapter 7

MAC Port Lockdown Maintenance

This chapter describes periodic maintenance procedures relating to Ethernet Port Security.

7.1 Monitoring for Alarms and Re-Locking Ports

Maintaining MAC Port Lockdown requires strict adherence to the procedures associated with the feature. Organizations implementing the feature may need to continually monitor the fault management application for alarms that indicate that the wrong equipment is connected to a port, or that a port is not secure.

NOTICE: For HP switches, relocking and re-enabling a port is required if the port was disabled due to an access attempt by a device with an unauthorized MAC address (see the procedures for relocking and re-enabling HP switches in MAC Port Lockdown Operation on page 43). You can view the MAC address of an unauthorized device on an HP switch by entering the following at the command line at the switch. The following command displays the Port, MAC Address, and Date/Time:

```
show port-security intrusion-log
```

After implementing MAC Port Lockdown, it is recommended that the fault management application be monitored for failover of redundant routers, to verify that MAC Port Lockdown is properly configured on the switch port connected to the second router (in a failover, the second router should become operable as the active router without generating security violation alarms).

For information about monitoring the fault management application, see the *Unified Event Manager* manual.

7.2 Software Patch Installation

The following table lists the software patches required to maintain Ethernet Port Security. Refer to the respective manuals for procedures to install software patches.

NOTICE: OS Patching does not apply to the K core or Express Trunking configurations. The RF Site products do not support patching. Instead, they require installing an entire new software release. For details, see the *Programming Software* documentation.

Table 7: Software Patches and References

Patch	ASTRO 25 System Manuals To See
HP switch OS patches	Switch manuals
RF equipment OS and application patches	RF site manuals
RADIUS server OS and application patches	*Authentication Services* manual
User Configuration Server (UCS) patches	*Private Network Management Servers* manual
VoyenceControl application patches	*Unified Network Configurator* manual

Patch	ASTRO 25 System Manuals To See
NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.	

Chapter 8

MAC Port Lockdown Troubleshooting

This chapter provides fault management and troubleshooting information relating to Ethernet Port Security.

8.1

Fault Management for MAC Port Lockdown on HP Switches

If an unauthorized device is connected to a MAC Port Lockdown enabled port on an HP switch, the switch port will be automatically disabled until manually re-enabled. (See MAC Port Lockdown Operation on page 43 for detailed instructions on re-locking and re-enabling the switch port.)

You can view the MAC address of an unauthorized device on an HP switch by entering the following at the command line at the switch. The following command displays the Port, MAC Address, and Date/Time:

```
show port-security intrusion-log
```

8.1.1

UEM Alarms for MAC Port Lockdown on HP Switches

If an unauthorized device is connected to a MAC Port Lockdown enabled port on an HP switch, notification of a security violation is sent to the Unified Event Manager (UEM).

For more details about the faults reported for Ethernet Port Security, refer to the *Unified Event Manager* manual.

8.1.2

Centralized Event Logging for HP Switch Port Security

If an unauthorized device is connected to a MAC Port Lockdown enabled port on an HP switch, notification of a security violation is recorded as a syslog event message. These messages are viewable from the Centralized Event Logging server, if present in the system, or locally at the device (for example, at the switch command line type `show log`).

For information on enabling/disabling Centralized Event Logging on HP switches, and viewing centralized logs, see the *Centralized Event Logging* manual.

8.2

Viewing Centralized Event Logging Records for GCP 8000 Site Controller/GPB 8000 Reference Distribution Module Port Security

The GCP 8000 Site Controller/GPB 8000 Reference Distribution Module's internal switch notifies Centralized Event Logging about the events listed in the following table.

NOTICE: All System Event Logs include the process ID, system date, system time, and device IP address. Refer to the *Centralized Event Logging* manual for instructions on viewing centralized event logs.

Table 8: System Events for GCP 8000 Site Controller/GPB 8000 Reference Distribution Module

System Event	Notes
Switch Port Connect A device is connected to an Ethernet port on the GCP 8000 Site Controller/GPB 8000 Reference Distribution Module's internal switch	Once the system is configured, the addition or removal of equipment on a port may indicate occurrence of an illegal activity.
Switch Port Disconnect A device is disconnected from an Ethernet port of the GCP 8000 Site Controller/GPB 8000 Reference Distribution Module's internal switch	Once the system is configured, the addition or removal of equipment on a port may indicate occurrence of an illegal activity.
Switch Port Security Change Port Security setting configuration parameter change	Once the system is configured, any changes made to the port settings may indicate that an intruder is attempting to gain access to the system (for example, changing a port from 802.1x to no security).
Switch Port Login Successful authentication by an 802.1x user	This creates an audit trail of who accessed the devices locally through an Ethernet switch. Interactive login/logout events include all command-line access to local management interfaces, including serial port access and network access with protocols such as serial command line, telnet, FTP, or SSH. This creates an audit trail of who has accessed the devices, both through the network or locally through a serial connection.
Switch Port Login (failed) Failed authentication by an 802.1x user	This creates an audit trail of who accessed the devices locally through an Ethernet switch. (See note above about interactive login/logout events)
Switch failure to apply security settings Port security settings could not be applied due to a hardware malfunction or inability to communicate with the switch hardware	This log implies that there is a mismatch between the persistent configuration of the switch and the actual switch port security settings. Failure to apply switch port configuration settings is also reported to the station log. Station logs can be viewed locally through the Configuration/Service Software (CSS). These logs are important to view because if there is a switch malfunction, fault traps, and system logs may not be transmitted from the switch to their destination in the network management subsystem.
Switch service port security settings disabled using the command line	This creates a log when the security settings are disabled for the service port through the command-line interface (telnet, SSH, or Serial Port).

Table continued…

System Event	Notes
Switch service port mirroring enabled using the command line	This creates a log when mirroring for the service port is enabled through the command-line interface (telnet, SSH, or Serial Port).
Switch service port mirroring disabled using the command line	This creates a log when mirroring for the service port is disabled through the command-line interface (telnet, SSH, or Serial Port).
RADIUS parameter change	Once the system is configured, any changes to the RADIUS configuration settings may indicate that an intruder is attempting to access the system.
	An example of change event for a RADIUS parameter would be changing the RADIUS shared secret or disabling the RADIUS server dead timer by changing its value from 5 to 0.

8.3 MAC Port Lockdown Faults

The following actions by service personnel can cause MAC Port Lockdown faults:

- Switching cables
- Replacing a host (such as a network management client, MCC 7500 console, and so on) with another host (such as a service laptop)

Avoiding these actions helps to prevent MAC Port Lockdown faults.

8.4 Link Failures

One link failure that may impact Ethernet Port Security is a fiber port hardware failure. In the unlikely case that the cable or mini-GBIC fail, the failure of the link between the two switches are reported in the central fault management system. You will need to replace the cable or mini-GBIC using the procedures in MAC Port Lockdown FRU/FRE Recovery Procedures on page 79.

The following are additional link failures that may impact Ethernet Port Security. They are covered in other manuals, as follows:

- **Link failure between RADIUS Authentication Server and the Ethernet Switch or internal switch in Remote Site Controllers** – For details about this link failure, refer to the *Unified Network Configurator* manual and the appropriate switch manuals.
- **Link failure between UNC application (VoyenceControl Server) and the Ethernet Switch or internal switch in Remote Site Controllers** – For details about this link failure, refer to the *Unified Network Configurator* manual and the appropriate device manuals.

NOTICE: The names EMC Ionix Network Configuration Manager and VoyenceControl are used interchangeably for this product.

Additional information on identifying link failures is available in the *Unified Event Manager* manual.

This page intentionally left blank.

Chapter 9

MAC Port Lockdown FRU/FRE Recovery Procedures

This chapter lists the Field Replaceable Units (FRUs) and includes replacement procedures applicable to Ethernet Port Security.

NOTICE: For lists of Field Replaceable Entities (FREs) of all models of HP switches used in ASTRO® 25 system, refer to the *System LAN Switches* manual.

9.1

Unlocking/Locking HP Switch Ports When Replacing Connected Devices

Prerequisites: Before performing this procedure, obtain the following information:

- The number of MAC addresses that are allowed to be learned by the port connected to the device that is being replaced. (For more information, see Determining the Number of MAC Addresses Learned by a Port on page 59).
- IP address of the new device. Contact your system administrator for the information.

When and where to use: Follow these steps to enable port security for a new device after replacing an old device, using the Cut-Through feature in VoyenceControl. Device replacement requires that the port to which the device is connected be unlocked, then relocked after the new device is connected.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

Procedure:

1. Perform one of the following procedures to log on to the switch and open a command line session:
   - Accessing the HP Switch Console with Telnet or SSH on page 55
   - Establishing Direct Console Access to the HP Switch on page 55
   - Logging on to an HP Switch with Cut-Through on page 56

   A command line window appears.
2. At the prompt, type `config`.
3. Type the following commands to disable the MAC Port Lockdown feature:
   a. `no port-security <port>`
   b. `interface <port>enable`
   c. `port-security <port> clear-intrusion-flag`

   The MAC Port Lockdown feature is disabled.
4. Connect the new device if it is not already connected.
5. Type the following commands to enable port security for the new device:

a `port-security <port>learn-mode static address-limit <numberMacAllowed> action send-Disable`

b `write memory`

The variable **<numberMacAllowed>** is the limit on the number of MAC addresses that can be learned. It can be from 1 to 31.

Port security is enabled for the new device.

6 Ping the device.

7 Validate MAC port lockdown. Follow the steps in Validating MAC Port Lockdown on HP Switches on page 68.

9.2

Locking/Unlocking a GCP 8000 Site Controller, GPB 8000 Reference Distribution Module or XHub Port When Replacing a Connected Device

For disabling/enabling MAC Port Lockdown when replacing devices connected to a GCP 8000 Site Controller's or GPB 8000 Reference Distribution Module's internal switch or when replacing a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module connected to an XHub's internal switch, see the following procedures:

- Enabling/Disabling MAC Port Lockdown on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with Site Wizards on page 49
- Enabling/Disabling 802.1x and MAC Port Lockdown for GCP 8000 Site Controller or GPB 8000 Reference Distribution Module with CSS on page 47
- Unlocking/Locking the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module Ethernet Port When Replacing a Site Gateway on page 51

9.3

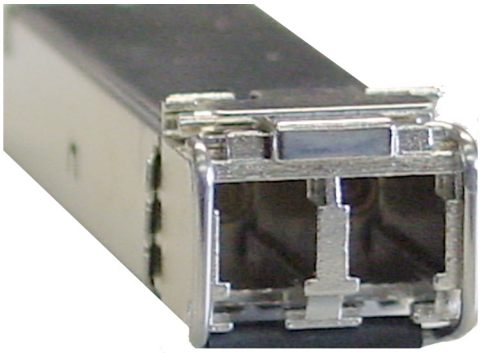
Fiber Connections Between HP Switches – Field Replaceable Units

The following table lists the FRUs that support the fiber connections between HP switches. This hardware must be ordered through the North America Parts Organization.

Table 9: Fiber Connections Between HP Switches – Field Replaceable Units

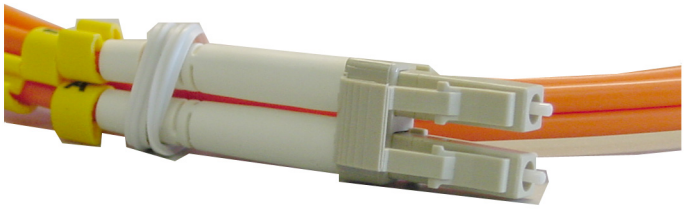
Part Number	Description	HP Switch Supported
CLN8490A	mini-GBIC (SX-LC transceiver)	• HP 3500 • HP 3800-48 • HP 26xx
CKN6906A	multi-mode fiber cable – LC(M) 3.3 FT	• HP 3500-48 • HP 3800-48 • HP 26xx

Figure 19: HP Switch Mini-GBIC Transceiver



HP_Switch_GBIC_Transceiver

Figure 20: HP Switch Fiber Cable



HP_Switch_Fiber_Cable

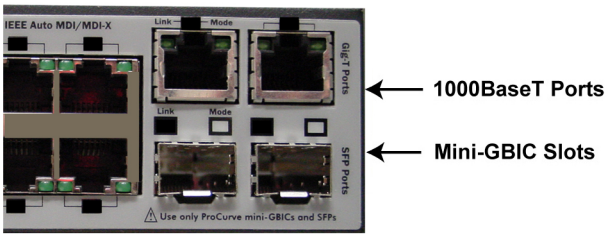
9.4

Mini-GBICs on HP 2620 and HP 3500/3800 Switches

HP 2620 switches have two Gigabit ports and two GBIC ports. When a mini-GBIC is installed in a slot, it operates independently of the RJ-45 ports. The mini-GBIC slots are not shared with the two 10/100/1000Base-T RJ-45 ports.

The following figure shows the slots where mini-GBICs are inserted on HP 26xx switches (an example of HP 2610) and the two 1000BaseT Ethernet ports.

Figure 21: HP 2610 Switch – Ethernet Ports and Slots for GBICs



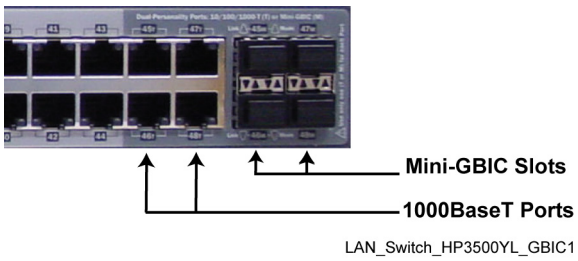
Switch_HP2610_GBIC1

NOTICE: The HP 2610 and 2620 switches have the same Ethernet ports and slots for GBICs.

HP 3500 switches have four Ethernet GIG-T (1000BaseT) ports and slots for fiber optic connections, which are associated with the corresponding Ethernet GIG-T (1000BaseT) ports. When a mini-GBIC transceiver is inserted into a fiber optic port, that port is enabled and the associated Ethernet GIG-T port is disabled. If the mini-GBIC is removed, the associated Ethernet port is automatically re-enabled but it needs to be reconfigured for operation on the LAN. Removing a mini-GBIC does not impact the operation of the remaining ports on the switch. Plugging in the GBIC brings the port back up.

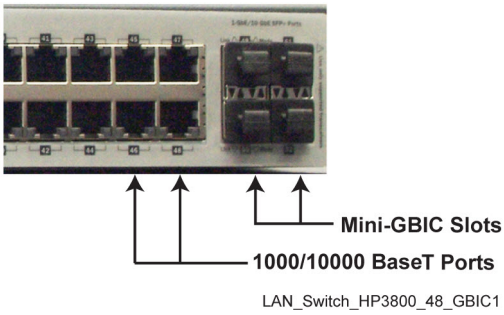
The following figure shows the slots for mini-GBICs on HP 3500 switches and the 1000BaseT Ethernet ports.

Figure 22: HP 3500 Switch – Example of Ethernet Ports and Slots for GBICs



HP 3800-48 switches have four SFP+ 1000/10000BaseT, full duplex ports along with 48 10/100/10000 non-POE full or half duplex ports for RJ-45 connections to network devices or installation of mini-GBIC for fiber-optic connections. Unlike HP 3500, HP 3800-48 switches have no dual personality, so inserting a mini-GBIC into a fiber optic port does not cause disabling an associated port.

Figure 23: HP 3800 Switch – Example of Ethernet Ports and Slots for GBICs



9.5 Replacing Mini-GBICs on HP 2620 and HP 3500/3800 Switches

Prerequisites: See Mini-GBICs on HP 2620 and HP 3500/3800 Switches on page 81 for considerations regarding Ethernet ports and mini-GBICs on HP switches.

Procedure:

1. Remove the fiber optic cables from their ports.
2. Perform one of the following steps to remove the mini-GBICs you are replacing:
   - If the mini-GBIC has a wire bail, lower the bail until it is approximately horizontal. Then using the bail, pull the mini-GBIC from the port.
   - If the mini-GBIC has a plastic tab or plastic collar, push the tab or collar toward the switch until you see the mini-GBIC release from the switch. Then pull it from the port.

   The LED on the associated 1000BaseT port turns on.
3. Hold the new mini-GBIC by its sides and gently insert it into one of the slots on the switch until the mini-GBIC clicks into place.

   The LED on the mini-GBIC port turns on. The LED on the associated 1000BaseT port turns off.
4. Repeat step 1 for all mini-GBICs.
5. Reload the configuration to all switches using the following command:

   `copy tftp start <IP address of TFTP Server><config file name>`

NOTICE: The TFTP server must be available and the configuration file must be in the root directory for the copy to be successful. The configuration file for the switch is created by Motorola Solutions. This helps ensure that the switch is configured properly and efficiently.

The configuration is loaded to the switch and the switch reboots.

6 Connect the fiber optic cable to the mini-GBIC port.

NOTICE: After aligning the notches on the cable connectors with the slots on the port, be sure to press the cable connector into the port until it snaps into place.

The corresponding link LEDs turn ON.

7 Repeat step 6 for the remaining ports on all trunked switches.

This page intentionally left blank.

Chapter 10

MAC Port Lockdown Reference

This chapter provides instructions that are useful when performing the MAC Port Lockdown procedures in this manual. The information in this chapter is covered in more detail in other manuals. This includes:

- Instructions for disabling 802.1x on a switch port, in case you need to use the port for MAC Port Lockdown procedures when network access is not available for 802.1x authentication. For more information, see the *802.1x Service Ports on Switches* manual.
- Procedures for enabling/disabling unused ports on HP switches, using the command line or pre-tested templates in the VoyenceControl component of Motorola's Unified Network Configurator (UNC) tool.
- General instructions for using pre-tested templates in VoyenceControl. Other templates used for MAC Port Lockdown are listed in the following sections in this manual:
  - Locking HP Switch Ports with a VoyenceControl Template on page 60
  - Disabling MAC Port Lockdown with a VoyenceControl Template on page 70

More detailed instructions for setting up and using VoyenceControl are provided in the *Unified Network Configurator* manual.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

10.1 Disabling 802.1x on a GCP 8000 Site Controller or GPB 8000 Reference Distribution Module Ethernet Port with the Serial Port

Prerequisites: Before performing this procedure, connect a technician's laptop to the serial port on the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module. The technician's laptop must have the Configuration/Service Software (CSS) installed on it.

When and where to use: Follow these steps to use the serial port on a GCP 8000 Site Controller/GPB 8000 Reference Distribution Module to change the Ethernet Security setting to “No Security”, and disable 802.1x authentication. However, network access is not available for 802.1x authentication at the port (for example, if a site gateway fails).

Procedure:

1. Launch the **CSS** application.
2. Click the **Connect to Device** button in the toolbar, or select **Tools** → **Connection Configuration** from the menu bar.

   The Connection Screen displays.
3. Select **Serial** as the Connection Type. (This causes the Serial Settings fields to un-gray in CSS.) Then select **Serial Port** and the appropriate **Baud Rate** (or leave the defaults). Click **Connect**.

   The connection is established.

4 Select **Tools → Service Port Configuration**.

The Service Port Configuration window appears.

5 Click **Unlock Service Port** to unlock the service port on the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module.

The service port status is set to “No Security”. After you write this configuration to the GCP 8000 Site Controller or GPB 8000 Reference Distribution Module, 802.1x will be disabled on the GCP 8000 Site Controller’s or GPB 8000 Reference Distribution Module’s Ethernet service port.

6 Click **Exit** to close the Service Port Configuration window.

10.2 Enabling/Disabling Ports on HP Switches with Local Access

When and where to use: An administrator with write privileges can use this procedure to enable or disable an Ethernet service port on an HP switch, using local access to the console port through a serial connection.

NOTICE: Faults may appear in the Unified Event Manager for HP switch 802.1x service ports that have no device connected to them. These faults can be removed if desired, by disabling these service ports when they are not being used by a service technician.

Procedure:

1 Connect a PC or terminal to the switch console port using the console cable that shipped with the switch.

NOTICE: If the PC or terminal has a 25-pin serial connector, first attach a 9-pin to 25-pin straight-through adapter to the PC end of the console cable.

2 Press ENTER two or three times until the command prompt appears.

3 Type in the password. Press ENTER.

The copyright information is displayed, followed by this message: `Press any key to continue`

4 Press any key.

The switch console Command Line Interface (CLI) prompt appears.

5 Put the switch into configuration mode:

a Type: `config`

b Press ENTER.

The prompt changes to `<switch>(config)#`. The switch is in configuration mode.

6 Perform the appropriate steps, depending on whether you want to enable or disable the port:

- If you want to enable the port, enter `interface <port> enable`
- If you want to disable the port, enter `interface <port> disable`

The port specified in the command is enabled or disabled, depending on your choice.

7 At the prompt, enter: `write memory`

The changes are saved.

8 Validate the change using the `show interfaces brief <port(s)>` command.

10.3

Enabling/Disabling Ports on HP Switches with VoyenceControl

All unused ports should be disabled before enabling Ethernet port security on the remaining ports. To disable unused ports on HP switches, use the process in Using a Motorola Solutions Template in VoyenceControl on page 87 and the information provided in the following table.

NOTICE: If faults appear in the Unified Event Manager for HP switch 802.1x service ports that have no device connected to them, these faults can be removed if desired, by disabling these service ports when not being used by a service technician. This section includes the information needed to disable the port and re-enable it from the VoyenceControl component of Motorola Solutions Unified Network Configurator.

Table 10: Template Information to Enable/Disable Unused Ports on HP Switches

Task You Are Performing	Subfolder Where Template is Located (under System > Motorola)	Name of the Template	Variable Fields That Require Input
Enabling port(s)	**HP**	Enable Port(s)	Port number(s) **Examples:** • For port number 3, type `3` • For port numbers a3, a5, a6, and a7, type `a3, a5-a7` You can enter up to 20 characters in the **Ports** field. If you reach the maximum of 20 characters (for example, when entering multiple non-contiguous port numbers), then you will need to perform the procedure again for the remaining port numbers.
Disabling port(s)	**HP**	Disable Port(s)	

10.4

Using a Motorola Solutions Template in VoyenceControl

When and where to use: Motorola Solutions provides pre-tested templates for changing the configuration of devices in an ASTRO® 25 system, through the VoyenceControl component of its Unified Network Configurator (UNC) tool. Follow these steps to change the configuration of a device in an ASTRO® 25 system using one of the Motorola Solutions templates available in VoyenceControl.

NOTICE: For information about setup and login, and additional ways to use templates, see the *Unified Network Configurator* manual.

Process:

1. Perform Logging into VoyenceControl on page 88.
2. Perform Accessing the Configlet Editor in VoyenceControl on page 88.
3. Perform Populating a Configlet with a Pre-Tested Template on page 89.
4. Perform Scheduling a Job in VoyenceControl on page 90.
5. Perform Viewing the Job Status in VoyenceControl on page 92.

6 Perform Viewing a Configuration Change in VoyenceControl on page 92.

Postrequisites:

NOTICE: After you perform the process, port security is enabled on port(s) locking to the learned MAC address(es), and an alarm message is sent when a violation occurs and the port is disabled (detection takes about 10 seconds). See Validating MAC Port Lockdown on HP Switches on page 68 to view port security details.

10.5 Logging into VoyenceControl

Procedure:

1 On the Network Management client where you set up VoyenceControl, double-click the **Internet Explorer** icon on the desktop to launch Internet Explorer.

2 In the Internet Explorer, enter the following URL:

`http://ucs-unc<Y>.ucs`

where:

<*Y*> is the number of the UNC server (`01` for the primary core UNC server, and `02` for the backup core UNC server).

A VoyenceControl client session launches and the Login dialog box appears.

3 Enter the User ID and Password, and then click **OK**.

The VoyenceControl main window appears.

10.6 Accessing the Configlet Editor in VoyenceControl

When and where to use: Follow these steps to access the Configlet Editor in the VoyenceControl component of Motorola's Unified Network Configurator tool.

NOTICE: For additional ways to use the Configlet Editor window, see the *Unified Network Configurator* manual.

Procedure:

1 Log into VoyenceControl.

The VoyenceControl main window appears.

2 In the navigation pane on the left side of the window, double-click **Astro 25 Radio Network**.

The selected network tree expands to display the Devices node.

3 In the navigation pane on the left side of the window, double-click **Devices**.

The Devices View appears. The list of devices and associated properties are displayed in the pane on the right side of the screen.

4 Right-click the desired device in the **Astro 25 Radio Network/Devices (view)** pane on the right side of the screen.

NOTICE: You can select multiple devices by holding the CTRL key while selecting the devices.

The context menu appears.

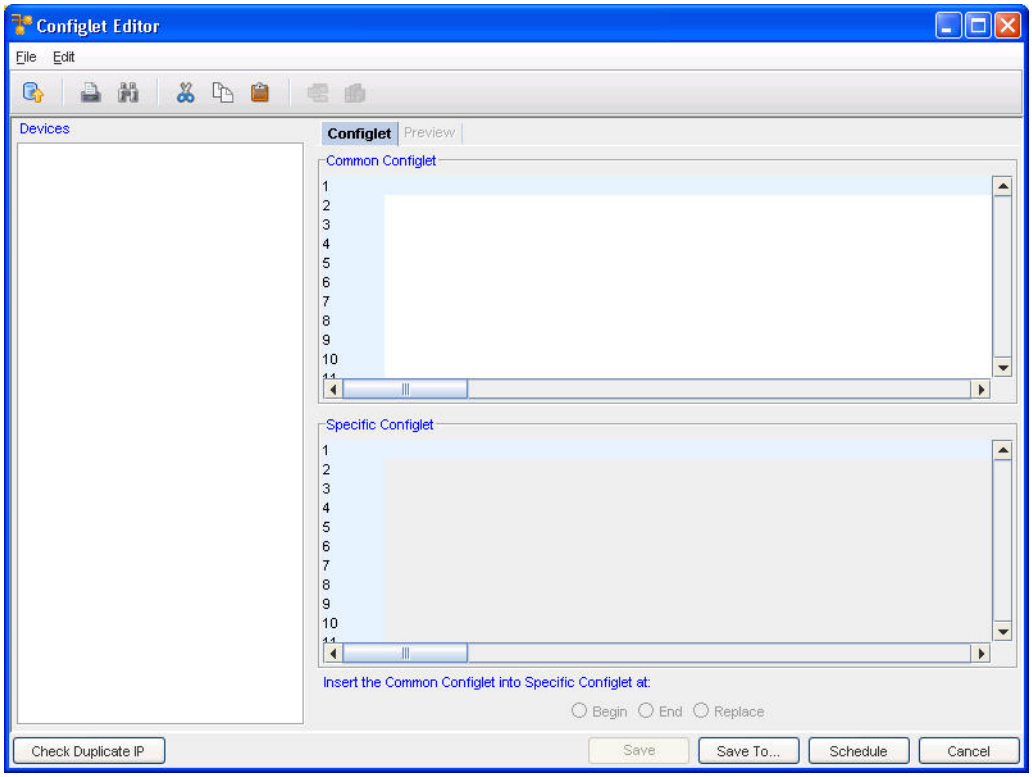
5 Select **Edit Device** → **Update Credentials**.

NOTICE: Make sure that the Mechanisms (protocols) appropriate for your organization's policies have been selected for this device on the Update Credentials window.

6 After closing the Update Credentials window, right-click the device again, and select **Editor** → **Configlet** from the context menu.

The following window appears.

Figure 24: VoyenceControl Configlet Editor Window – Example



10.7 Populating a Configlet with a Pre-Tested Template

When and where to use: Follow these steps to use a template to populate a Configlet in the VoyenceControl component of Motorola's Unified Network Configurator tool.

NOTICE: For additional ways to use templates, see the *Unified Network Configurator* manual.

Procedure:

1 Access the Configlet Editor window in VoyenceControl.

2 Click inside the text box at the top of the **Configlet Editor** window.

The **Insert Template** icon becomes active in the tool bar of the Configlet Editor window.

3 Click the **Insert Template** icon.

The **Select Item** dialog box appears.

4 Click the folder icon at the top of the dialog box, to the right of the **Look in** field.

Continue to click this icon until the **System** folder displays in the list of folders on the Select Item dialog box.

5 In the list of folders on the Select Item dialog box, double-click the **System** folder, then double-click the **Motorola** folder.

6 Double-click the subfolder that contains the template you need.

A list of templates displays on the **Select Item** dialog box.

7 Double-click the template you need from the list.

One of the following events occurs:

- If you are not required to input values, you are returned to the **Configlet Editor** window.
- If the template requires you to input values for variable(s), the **Template Variable Substitution** window displays a field for entering each value. You must enter a value in each field on this window and click **OK**, before you are returned to the Configlet Editor window.

When you are returned to the **Configlet Editor** window, the configuration lines generated by the template are displayed.

10.8 Scheduling a Job in VoyenceControl

When and where to use: After using the Configlet Editor window for a selected device, follow these steps in the VoyenceControl component of Motorola's Unified Network Configurator tool, to push the contents of the Editor window to the device.

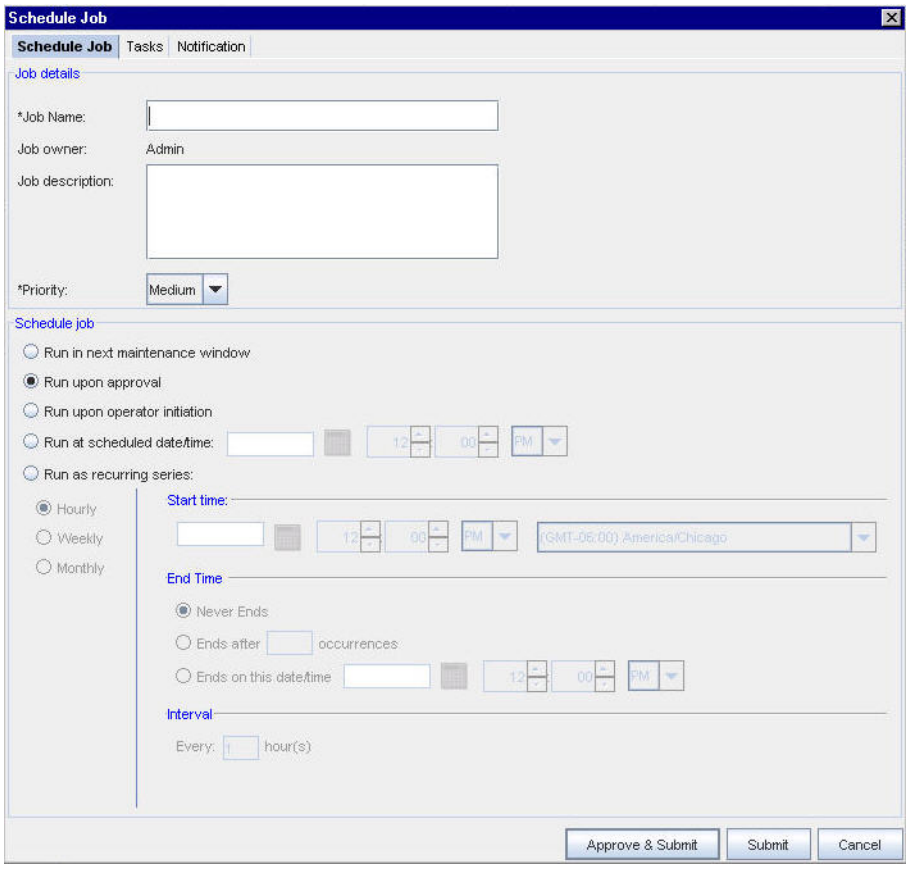
NOTICE: For additional ways to use the Schedule Job window, see the *Unified Network Configurator* manual.

Procedure:

1 Click the **Schedule** button at the bottom of the Editor window.

The following window appears.

Figure 25: VoyenceControl Schedule Job Window – Example



2 On the **Schedule Job** tab, enter a **Job Name**.

3 On the **Tasks** tab, ensure that the following defaults are used:

   1 **running-configuration**

   2 **Copy to Start**

   3 **Pull Configs**

   NOTICE: Verify that the selected Mechanism is appropriate for your organization's policies.

4 Click the **Approve & Submit** button or click the **Submit** button, depending on your permissions.

   NOTICE:

   - If you clicked the **Approve & Submit** button, the Schedule Job window closes and the job status can be viewed using **Tools** → **Schedule Manager** available from the menu bar in the VoyenceControl main window.
   - If you clicked the **Submit** button, the status of the job is Pending. You can approve Pending jobs in the Schedule Manager window.

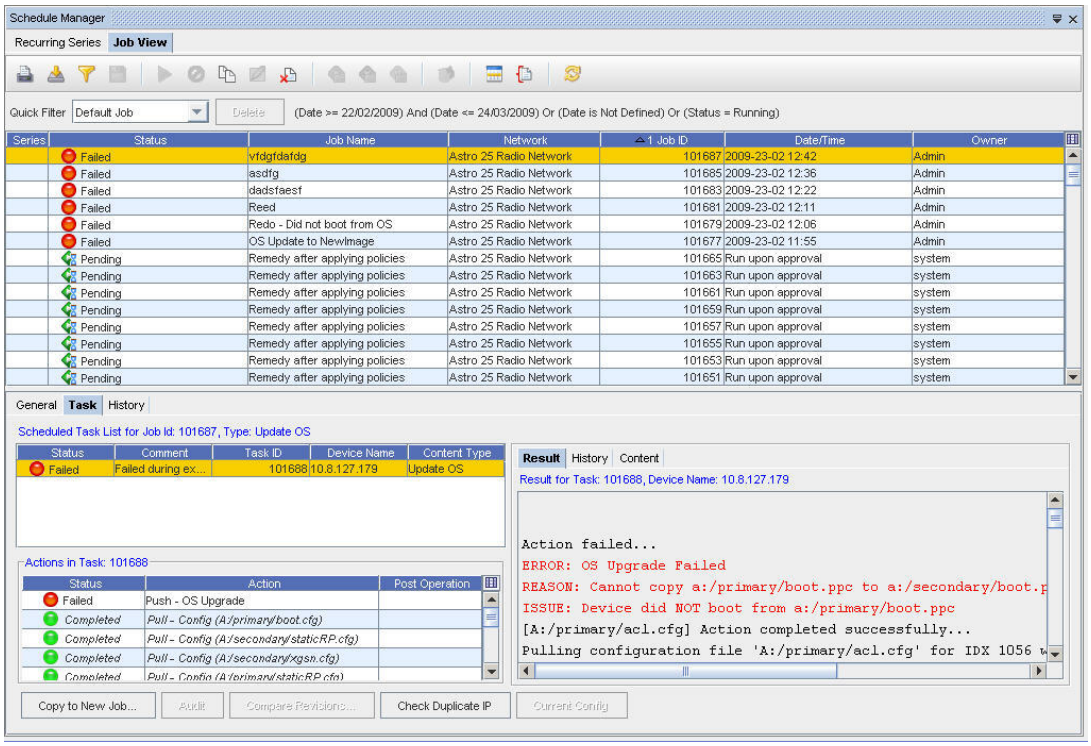
   The system runs the updated configuration.

5 Close the Editor window.

10.9
Viewing the Job Status in VoyenceControl

After scheduling a job in the VoyenceControl component of Motorola's Unified Network Configurator tool, you may view the job status. The status is displayed in the Schedule Manager window available from **Tools → Schedule Manager** from the menu bar.

Figure 26: Schedule Manager Window – Example



NOTICE: For additional ways to use Schedule Manager, see the *Unified Network Configurator* manual.

10.10
Viewing a Configuration Change in VoyenceControl

When and where to use: Follow these steps to view a configuration change for a device in the VoyenceControl component of Motorola's Unified Network Configurator (UNC). This procedure verifies that a configuration change was pushed to a device and was then pulled into UNC configuration records.

NOTICE: For additional information on how to use the UNC, see the *Unified Network Configurator* manual.

Procedure:

1. At the **Schedule Manager** window, press F5 to update the view.
2. Select a device for which you want to view a configuration change.
3. From the device properties area that displays in the lower half of the screen, select the **History** tab.
4. Compare two configurations as follows:
   a. Select the two configurations you want to compare from the list (in this case, you want to compare the two most recent configurations in the list).

b Click the **Compare Device Revision Configs** icon in the toolbar.

10.11

Viewing Enabled/Disabled State for HP Switch Ports with a Saved Command

When and where to use: If configurations have been updated in the VoyenceControl component of Motorola's Unified Network Configurator (using a scheduled job, or manually using **Pull Config**), you can perform the following procedure. This way you can determine if HP switch ports are enabled or disabled.

NOTICE: For information on setup, login, and additional ways to use VoyenceControl, see the *Unified Network Configurator* manual.

Procedure:

1. Log into VoyenceControl.

   The VoyenceControl main window appears.

2. In the navigation pane on the left side of the window, double-click **Astro 25 Radio Network**.

   The selected network tree expands to display the Devices node.

3. In the navigation pane on the left side of the window, double-click on **Devices**.

   The Devices View appears. The list of devices and associated properties are displayed in the pane on the right side of the screen.

4. Right-click the desired switch in the Devices View pane on the right side of the screen.

   The context menu appears.

5. Select **Saved Commands** from the context menu.

   The Select Item dialog box displays.

6. Click the folder icon at the top of the dialog box, to the right of the **Look in** field. Continue to click this icon until the **System** folder displays in the list of folders on the Select Item dialog box.
7. In the list of folders on the Select Item dialog box, double-click the **System** folder, then double-click the **Motorola** folder, and then double-click the **HP** folder.

   A list of saved commands displays on the Select Item dialog box.

8. Double-click the saved command named **Show All Ports Interface**.

   A progress window appears. After approximately 30 seconds, the Results dialog box appears. If the command is executed successfully, the switch appears in the **Successful Results** list.

9. Click the device in the **Successful Results** list.

   The Results field displays which ports are up and which ports are down.

This page intentionally left blank.