System Release 7.17
ASTRO ® 25
INTEGRATED VOICE AND DATA

S6000 and S2500 Routers

SEPTEMBER 2020

MN003363A01-B

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.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

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.

Contact Us

The Solutions Support Center (SSC) is the primary contact for technical support included in your organization's service agreement with Motorola Solutions.

Service agreement customers should be sure to call the SSC in all situations listed under Customer Responsibilities in their agreement, such as:

- Before reloading software
- To confirm troubleshooting results and analysis before taking action

Your organization received support phone numbers and other contact information appropriate for your geographic region and service agreement. Use that contact information for the most efficient response. However, if needed, you can also find general support contact information on the Motorola Solutions website, by following these steps:

1. Enter motorolasolutions.com in your browser.
2. Ensure that your organization's country or region is displayed on the page. Clicking or tapping the name of the region provides a way to change it.
3. Select "Support" on the motorolasolutions.com page.

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 or title of the section with the error
- A description of the error

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to https://learning.motorolasolutions.com to view the current course offerings and technology paths.

Document History

Version	Description	Date
MN003363A01-A	Original release of the *S6000 and S2500 Routers* manual.	November 2016
MN003363A01-B	Updated section: - Completing the Configuration on page 40	September 2020

Contents

List of Figures

List of Tables

List of Processes

List of Procedures

About S6000 and S2500 Routers

This manual provides an introduction to the S6000 and S2500 routers. The manual provides information relating to the installation, configuration, and management of the S6000 and S2500 routers as used in various network locations.

What is Covered In This Manual?

This manual contains the following chapters:

- S6000 Introduction, Installation, and Configuration on page 27 provides a high-level description of the S6000 router and describes its features.
- S2500 Introduction, Installation, and Configuration on page 66 provides a high-level description of the S2500 router and describes its features.
- ASTRO 25 Master Site on page 110 provides information on routers in an ASTRO® 25 Master Site.
- ASTRO 25 Repeater Site on page 138 provides information on the S2500 router in an ASTRO® 25 Repeater Site.
- ASTRO 25 HPD Site on page 144 provides information on the S2500 router in an ASTRO® 25 High Performance Data (HPD) Site.
- ASTRO 25 Dispatch Console Subsystem on page 157 provides information on the routers in an ASTRO®25 Dispatch Console subsystem.
- ASTRO 25 IP Simulcast Subsystem on page 163 provides information on the routers in an ASTRO® 25 IP Simulcast subsystem.
- ASTRO 25 Conventional Master Site (K Core) on page 197 provides information on the S6000 router in an ASTRO® 25 K core Conventional Master Site.
- ASTRO 25 Customer Enterprise Network on page 200 provides information on the S6000 routers in an ASTRO® 25 Customer Enterprise Network.
- ASTRO 25 Centralized Conventional Sites on page 209 provides information on the S2500 routers in ASTRO® 25 system conventional architectures.
- ASTRO 25 Interoperability on page 235 provides information on the S2500 used at the ISSI.1 site.
- ASTRO 25 Circuit Simulcast Subsystem on page 237 provides information on the routers in an ASTRO® 25 Circuit Simulcast subsystem.
- System Routers Reference on page 245 describes the router platforms and nomenclature.
- System Routers Disaster Recovery on page 248 provides references and information that enable you to recover a router in the event of a failure.

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 to view the current course offerings and technology paths.

Related Information

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides information relating to the installation, configuration, and management of the S6000 and S2500 routers as used in various network locations. This manual 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.
System Gateways – GGM 8000	Provides information relating to the installation, configuration, and management of the GGM 8000 as used in various network locations.
MNR S2500 and MNR S6000 router hardware user guides and EOS software manuals	Available on the Motorola Online website: https://businessonline.motorolasolutions.com To access the manual, select **Resource Center** → **Product Information** → **Manuals** → **Network Infrastructure** → **Routers and Gateways**. The following manuals are available: • *Enterprise OS Software Reference Guide* • *Enterprise OS Software User Guide* • *Motorola GGM 8000 Hardware User Guide* • *Motorola Network Router (MNR) S2500 Hardware User Guide* • *Motorola Network Router (MNR) S6000 Hardware User Guide*

Chapter 1

S6000 Introduction, Installation, and Configuration

This chapter provides a high-level description of the S6000 router and describes its features.

NOTICE: The GGM 8000 can be used as a replacement for the following S6000 routers employing Ethernet site links: S6000 GGSN (GPRS Gateway Support Node), S6000 Gateway Router, S6000 Core router, S6000 Exit router, and S6000 Core/Exit router. See the *GGM 8000 System Gateway* manual for details.

1.1 S6000 Physical Description

This section describes the physical hardware for the Motorola Network Router (MNR) S6000 router.

1.1.1 Front Panel Description – S6000

The S6000 router is available without modules or with variations of the I/O modules.

The front panel has the following connectors and ports:

Ethernet connectors

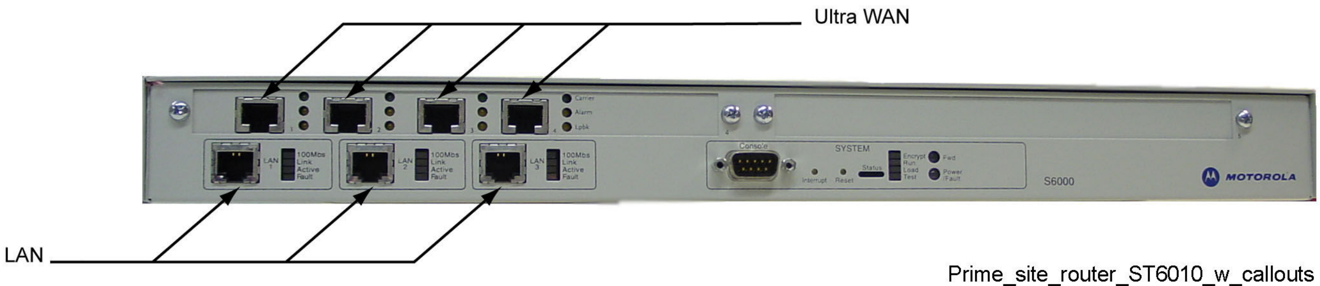
Three Ethernet ports (RJ-45 connectors) provide the Local Area Network interface. These ports are labeled LAN 1, LAN 2, and LAN 3.

NOTICE: The third Ethernet port is used for Ethernet LAN connectivity if the Flexible Ethernet Connectivity feature is implemented on the system.

Console port

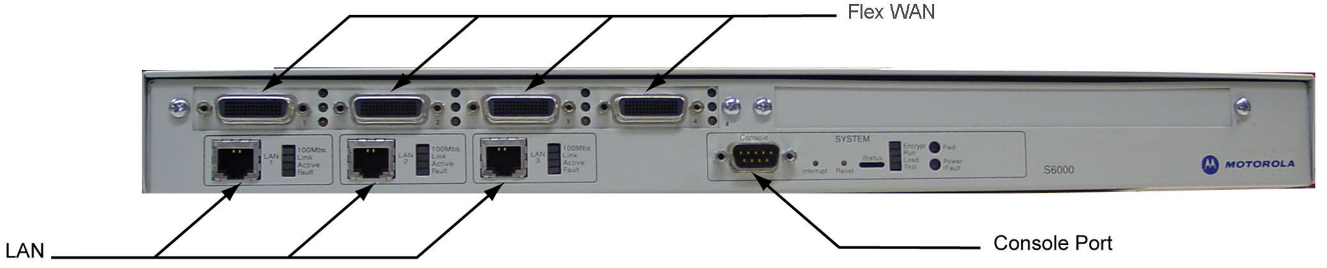
The DB9 connector is used to connect a local terminal, such as a laptop, to the router for service

Figure 1: S6000 Router with an ST6010 (UltraWAN) Module



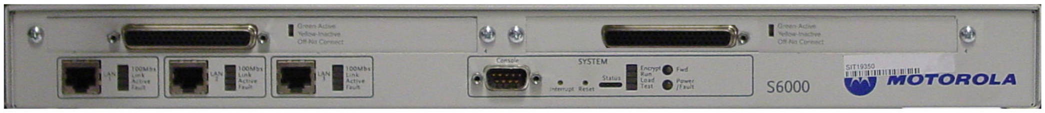
Prime_site_router_ST6010_w_callouts

Figure 2: S6000 Router with an ST6011 (FlexWAN) Module



Gateway_Router_ST6011_w_callouts

Figure 3: S6000 Router with a 12-Port T1/E1 Modules



S6000_w_2relay_pnls

1.1.2
Rear Panel Description – S6000

This section describes the elements on the rear of the S6000 router.

The rear panel contains:

Ground screw

Used to connect a protective ground wire.

Power receptacles

Depending on the base unit model, power supplies of one or two internal power receptacles are:

- S6000 base units with model numbers CLN1780A and higher have a single power supply.
- S6000 base units with model numbers lower than CLN1780A have redundant power supplies.

NOTICE: The base unit model number is listed on the label on the rear of the router.

1.1.3
S6000 Router – Physical Specifications

Table 1: S6000 Router – Physical Specifications

S6000 Router	Specifications
Physical dimensions	Height: 4.3 cm (1.7 in.)
	Width: 30.5 cm (12.0 in.)
	Depth: 43.0 cm (16.9 in.)
Weight	4.54 kg (10 lb)

1.1.4 S6000 Router – Environmental Specifications

You must adhere environmental requirements when installing the router.

IMPORTANT: The S6000 router requires proper ventilation and space to accommodate cabling requirements.

Table 2: S6000 Router – Environmental Specifications

Environmental Characteristic	Minimum Requirement	Maximum Requirement
Operating Temperature	0° C (32° F)	50° C (122° F)
Non-operating Temperature	-30° C (-22° F)	60° C (140° F)
Operating Altitude	N/A	3,048 m (10,000 ft)
Non-operating Altitude	N/A	12,192 m (40,000 ft)
Relative Humidity – Operating	5% non-condensing	95% non-condensing
Relative Humidity – Non-operating	5% non-condensing	95% non-condensing
Power Requirements	N/A	60 W (S6000 CWR Configuration), or 80 W (S6000 Non-CWR Configuration)
Heat Dissipation	N/A	136 Btu/hr, 205 Btu/hr, or 273 Btu/hr

1.2 S6000 Router Types

Routers perform network transport functions for the control of audio, data, and network management traffic used by the system.

Transport functions include:

- Directing Ethernet traffic (gateway routers)
- Conducting protocol conversions (core and exit routers)
- Joining subnets

The following table lists transport functions for the ASTRO® 25 system that the routers provide.

Table 3: Routers by System Location and Function

Location	Function	Comments
Master site	Gateway router	Provides functional support for the zone controller, packet data gateway (PDG), and network management system routing.
	Core router	Handles network traffic between the master site and the sites associated with that master site (intrazone support only).
	Exit router	Handles network traffic between master sites (InterZone support only).
	Core/Exit router	Combines the roles of the core and exit routers. Dual Function: Intra-Zone traffice (Zone-to-Site) and Inter-Zone traffic (Zone-to-Zone). Supports only Ethernet site links.

Location	Function	Comments
	GGSN router	(GPRS Gateway Support Node router) Handles network traffic between the Motorola Solutions radio network infrastructure and external networks to support data services.
Conventional master site	GGSN router	(GPRS Gateway Support Node router) Handles network traffic between the Motorola Solutions radio network infrastructure and external networks to support data services.
Network security	Border router	Provides an interface from your enterprise network to the peripheral network of the Motorola Solutions radio network infrastructure.
	Peripheral network router	Connects various peripheral networks together and expands border router access capability to the peripheral network for your enterprise network.
Circuit Simulcast Prime Site	Circuit Simulcast prime site router	Handles network traffic between a simulcast subsystem prime site and the link to the master site. Distributes voice, control, and network management traffic to the appropriate devices on the prime site network.
IP Simulcast Prime Site	IP Simulcast prime site router	Handles network traffic between a simulcast subsystem prime site and the link to the master site. Distributes voice, control, and network management traffic to the appropriate devices on the prime site network.
	IP Simulcast remote access router	Directs all control, voice, and network management traffic between the prime site LAN and the subsites. The remote access router facilitates the connectivity to the subsites as well as fast convergence on the interfaces (T1/E1 or Ethernet) when failures occur.
Trunking Subsystem	Trunking subsystem prime site router	Handles network traffic between a trunking subsystem prime site and the link to the zone core. Distributes voice, control, and network management traffic to the appropriate devices on the prime site network.
	Trunking subsystem remote access router	Directs all control, voice, and network management traffic between the prime site LAN and the subsites. The remote access router facilitates the connectivity to the subsites as well as fast convergence on Ethernet links when failures occur.
Dispatch Console Site Subsystem	Dispatch Console Site router	Handles network traffic between a Dispatch Console site and the link to the master site. Distributes voice, control, and network management traffic to the appropriate devices on the Dispatch Console site network. This type of router can also be the S2500 model or a GGM 8000 model. For information regarding GGM 8000, see the *GGM 8000 System Gateway* manual.

For more information about routing, see the *Cooperative WAN Routing* manual.

1.2.1 Information Assurance Features Overview

The applicable Information Assurance (IA) features are included in different appropriate manuals.

NOTICE: Border Router and Peripheral Network Router do not have IA configurations, for example, they do not need SNMPv3 for fault management.

Table 4: Information Assurance Features

IA Feature	Related Manual
Router encryption and authentication (to filter traffic based on originating host), including Router Encryption Card Configuration	*Link Encryption and Authentication* manual
SSH (for secure data transfer)	*Securing Protocols with SSH* manual
Remote Authentication Dial-In User Service (RADIUS) client configuration	*Authentication Services* manual
SNMPv3 for fault management in the Unified Event Manager (UEM)	*SNMPv3* manual
Router Access Control Lists (ACLs) to encrypt links	*Information Assurance Features Overview* manual
Centralized Event Logging	*Centralized Event Logging* manual

1.3 S6000 Installation

Installation procedures for S6000 routers are common to all S6000 router applications.

1.3.1 Installing an S6000 Router in a Rack

Routers are rack-mounted to provide easy access during installation and cabling.

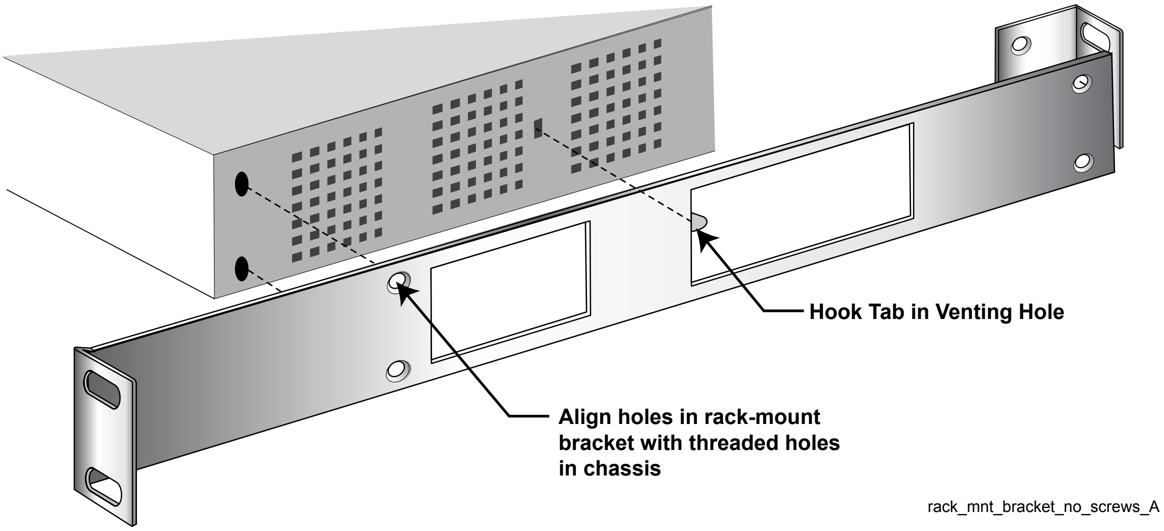
Prerequisites: Prepare:

- Two rack-mount brackets
- Four 8/32 flathead Phillips screws
- Eight TORX screws
- Four TORX screws

Procedure:

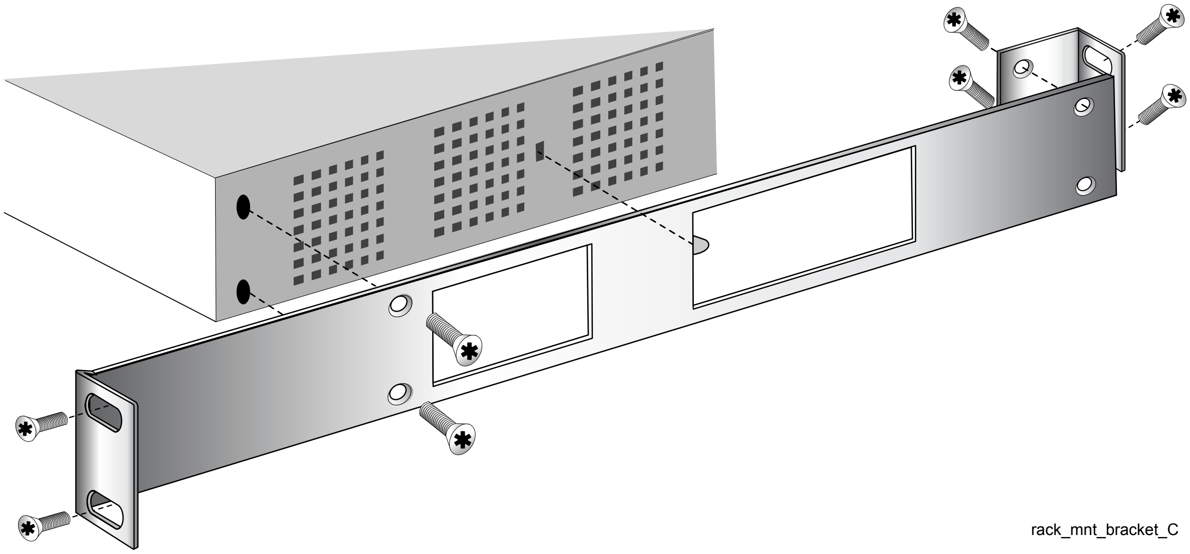
1. Hook the tab of one of the rack-mount brackets into a venting hole on the side of the router chassis so that the holes on the bracket are aligned with the threaded holes on the chassis, as shown in the following figure.

Figure 4: Hooking the Rack-Mounting Bracket


Hook Tab in Venting Hole
Align holes in rack-mount bracket with threaded holes in chassis
rack_mnt_bracket_no_screws_A

2 Secure the rack-mount bracket to the side of the chassis using two 8/32 flathead Phillips screws using a Phillips screwdriver, as shown in the following figure. Torque to 15 lb/in.

Figure 5: Securing the Brackets



3 Repeat step 1 and step 2 to attach the other rack-mount bracket to the other side of the router chassis.

4 Hold the chassis between the poles of the rack and attach the front of the brackets to the rack on each side with four TORX screws using a T-25 TORX screwdriver. Torque to 60 lb/in.

⚠ **CAUTION:** Using fewer than two screws on each side to secure the brackets to the rack may cause the router to fall and sustain damage not covered by the warranty.

5 Attach the rear mount brackets to each side of the rear of the brackets using four TORX screws using a T-25 TORX screwdriver. Torque to 60 lb/in.

6 Attach the rear of the brackets to the rack on each side with four TORX screws using a T-25 TORX screwdriver. Torque to 60 lb/in.

Postrequisites: Before connecting the routers, ensure that you have the required cabling and connectors.

CAUTION: Use only Category five unshielded twisted pair (or higher) cabling and connectors. Motorola Solutions has engineered this system to meet specific performance requirements. Using other cabling and connectors may result in unpredictable system performance or catastrophic failure.

1.3.2 S6000 Router – Power Connections

The S6000 router connects to a standard 120 V power outlet source. You must consider power specifications when installing the router.

IMPORTANT: Before servicing the S6000 router, always disconnect it from the power source. The power source connection should be the last connection established when installing the S6000 router.

NOTICE: Use one circuit breaker per router.

Table 5: S6000 Router – Power Connections

Voltage	Consumption
100–240 V AC	60 W AC (each router)

1.3.2.1 Connecting the S6000 Router to the Power Source

The S6000 router has one or two internal power supplies on the rear panel, depending on the base unit model.

Prerequisites: Install the router on your system.
Determine the number of power supplies:

- For the base unit, check the part number on the label on the rear of the router.
- S6000 routers with redundant power supplies have model numbers lower than CLN1780.

When and where to use: Power up the router and verify that it is working.

Procedure:

1. Connect the **female** end of a power cable to one of the power receptacles on the rear panel of the router.
2. Connect the **male** end of the power cable to the appropriate power source outlet (such as the AC outlet).
3. If the S6000 is configured with redundant power supplies, repeat these steps for the second power receptacle.

   IMPORTANT: If one of the receptacles is open, a warning-level SNMP trap is generated. To take full advantage of the redundant power supplies in the router, connect the second power receptacle to a power source on a different circuit.
4. Verify that the power LED is on.

The power-up process takes a few seconds. Successful completion of the process is indicated with the LEDs on the front panel of the router.

NOTICE: An appropriate device must be connected to the router, and powered on for the Local Area Network (LAN) LEDs to display properly.

See S6000 Troubleshooting on page 48 for further details about the LEDs.

NOTICE: Using a UPS backup power supply is recommended.

1.3.3 Connecting the Router to Ground

Prerequisites: Locate the grounding (earthing) screw on the chassis. Some network topologies require that a grounding screw, separate from the AC ground, be provided on the chassis of the networking equipment.
Prepare:

- 3-prong grounding plug to connect to the AC system. If further grounding is required, use the grounding screw.
- Ground wire (minimum #6 AWG wire)

  NOTICE: If the length of the grounding wire must exceed 4 meters before it is terminated, grounding wire larger than #6 AWG is required. Refer to *Standards and Guidelines for Communication Sites*, also known as the *R56* manual, for details.
- UL-listed ring lug

Procedure:

1. Terminate one end of a ground wire with a UL-listed ring lug.
2. Attach the ring lug of the ground wire to the ground screw on the rear panel of the router.
3. Terminate the other end of the ground wire on a permanently connected protective grounding conductor or Rack Grounding Bar (RGB).

1.4 S6000 Configuration

This section provides configuration information for the router.

1.4.1 Router Software and Configuration Files Installation

The router's Enterprise Operating System (EOS) software and configuration files are installed at the factory. No additional installation is required.

If you replace a router, EOS software and configuration files have to be loaded on the new router after it is installed in the rack. If a firmware downgrade is necessary due to an MNR replacement, check the version of the firmware. Additional steps may be required depending on the firmware version. See Performing a Firmware Downgrade on page 250.

- If the router has no connectivity to the Unified Network Configurator (UNC) through the network, reload the files locally at the router using a service laptop and the configuration files provided by Motorola Solutions.
- If the router has connectivity to the UNC through the network, reload the files from the UNC, provided they were "pulled" to this application from the router before the failure.

For routers that are managed by UNC, see the *Unified Network Configurator* manual to learn about updating EOS images and software.

1.4.2 Router Configuration

This process explains how to load a router configuration file on a new router.

1.4.2.1 Configuration Prerequisites

You need to obtain certain items before you load a configuration file on a new router.

Table 6: Configuration Prerequisites

Prerequisite	Details
PC with a terminal emulation program and a 3com TFTP server application	Service technician's laptop
Ethernet crossover cable	To establish a LAN connection between the PC and the router
DB9 null modem cable	To establish console access between the PC and the router
Appropriate router configuration file for the router you are installing or replacing: `boot.cfg` (required), `StaticRP.cfg` and `acl.cfg` (if used)	Use the customized configuration files on the media device provided for your system by Motorola Solutions or backed up on your PC. For help in locating these files, contact your system administrator.
IP address for the router	Contact your system administrator for this information.
Account logins and passwords	Contact your system administrator for this information.

Configuration Prerequisites – Cautions and Notes

⚠ **CAUTION:** Do not tamper with the factory configuration settings for these devices. This includes software configuration, firmware release, and physical connections. Motorola Solutions has configured and connected these devices to meet very specific performance requirements. Tampering with these devices may result in unpredictable system performance or catastrophic failure.

NOTICE: Routers are configured at the factory. No additional configuration is required other than restoring the routers in the event of a break-fix situation. Field configuration of site routers is allowed, but you must contact the Motorola Solutions Support Center (SSC) for the configuration of routers at the master site or for the configuration of transport network devices at the remote site.

1.4.2.2 Configuring the S6000 Router

This process explains how to load a router configuration file on a new router.

Prerequisites: If necessary, contact your system administrator for prerequisite information.

When and where to use: Motorola Solutions routers are shipped from the factory with the appropriate Enterprise OS (EOS) installed. If you replace a router in the field and it is not possible to configure the replacement router at the factory, or if you need to load a router configuration file onto a new router during installation, follow this process.

NOTICE: Note that in ASTRO/LTE CEN systems the Border Router requires a configuration file established manually using a text editor to meet specific requirements for each Customer Enterprise Network (CEN). See your Motorola Solutions field support representative. For details concerning Border Routers in ASTRO/LTE CEN configuration see Border Router – Functional Description on page 200.

Process:

1. Review the configuration prerequisites. See Configuration Prerequisites on page 35.
2. Determine the set of configuration files that is needed. See Configuration Files – S6000 on page 36.
3. Configure the IP address. See Configuring the IP Address and Workstation Connections on page 37.
4. Set up the 3Com TFTP application. See Configuring TFTP on page 38.
5. Transfer the configuration file. See Transferring the Router Configuration File on page 39.
6. Verify that the router rebooted and is running the new configuration. See Verifying the New Configuration on page 40.
7. Complete the router configuration. See Completing the Configuration on page 40.

1.4.2.3
Configuration Files – S6000

Different sets of configuration files applies for different S6000 router types.

S6000 Router		Configuration Files Set
Border Router		boot.cfg acl.cfg
Peripheral Network Router		boot.cfg acl.cfg
Master Site Routers:		boot.cfg acl.cfg StaticRP.cfg
	Core Router	
	Exit Router	
	Core/Exit Router	
	Gateway Router	
Circuit Simulcast-based Prime Site Router		boot.cfg acl.cfg StaticRP.cfg
IP Simulcast Prime Site Routers:		
	Prime Site Router	boot.cfg acl.cfg StaticRP.cfg
	Remote Site Access Router	boot.cfg acl.cfg

S6000 Router		Configuration Files Set
Trunking Subsystems		
	Prime Site Router	boot.cfg acl.cfg StaticRP.cfg
	Remote Site Access Router	boot.cfg acl.cfg
GGSN Router		boot.cfg acl.cfg xgsn.cfg
Dispatch Console Site Router		boot.cfg acl.cfg StaticRP.cfg
Conventional Master Site (K core) GGSN Router		boot.cfg acl.cfg xgsn.cfg

1.4.2.4

Configuring the IP Address and Workstation Connections

You have to perform certain steps to configure the IP address for the router and connect it to a service workstation or laptop. Configure the IP address also when you replace a router in the field and load the router configuration file on a new router during installation.

Prerequisites: Install the router in the rack and ground it.
Connect the router to a power source and power it up.

Obtain:

- Ethernet crossover cable
- Null modem cable
- PC with a terminal emulation program

When and where to use: If you load a configuration file that changes the system IP address on an MNR router, the SNMPv3 credentials must be re-established with that router. Therefore, if SNMPv3 users were configured on the router before the system IP address change, you must issue the **ResetV3** command to reset the SNMPv3 data, then reconfigure the SNMPv3 users with the appropriate privilege levels. For details, see “Configuring MNR Routers and GGM 8000 Gateways for SNMPv3” in the *SNMPv3* manual.
After performing the **ResetV3** command to reset SNMPv3 data on an MNR router or GGM 8000 gateway, make sure to clear the USM cache. For details, see the “Accessing and Executing Existing Saved Commands” section in the *Unified Network Configurator* manual.

Clearing the cache does not apply to routers that do not use SNMP, which includes Border Routers or Peripheral Network Routers.

Procedure:

1 Assign the Ethernet port on the PC being used to perform the configuration:

- **IP Address**: 20.0.0.1
- **Subnet Mask**: 255.255.255.0

2 Connect the following cables between the PC and the router:

- Ethernet crossover cable between the Ethernet port on the PC and the LAN 1 port on the front of the router.

  NOTICE: The crossover cable crosses over pins 1 and 2 to pins 3 and 6.

- Null modem cable between the serial port on the PC and the console port on the router.

3 Power up the router and establish communication using a terminal emulation program, such as ProComm+ or HyperTerminal.

4 In the terminal emulation program, perform the following actions:

a Enter: `9600 baud rate`

b Enter: `8 bit`

c Enter: `No parity`

d Enter: `1 stop bit`

Press ENTER several times until the `NetLogin:` prompt appears.

5 At the `NetLogin:` prompt, type the default account name, **`root`**. Press ENTER.

6 At the `Password:` prompt, press ENTER. No password is necessary on an unconfigured router.

The `EnterpriseOS#` prompt appears.

NOTICE: The password for unconfigured routers is not defined.

7 Verify that the router is unconfigured (no IP addresses are assigned to any of the ports) by typing `sh -ip net`. Press ENTER.

NOTICE: If there are any IP addresses defined, you must use the:
`del !`***`<portlist>`*** `-ip net` ***`<ip address>`***

command to delete them before continuing with this procedure.

8 To configure the IP address for the router, type the following command and press ENTER:

```
setd !1 -ip net = 20.0.0.2 255.255.255.0
```

NOTICE: The character after `setd !` is a number 1 (one).

NOTICE: The IP addresses assigned in this procedure to the PC's Ethernet port and to the router have been chosen so that the router's IP address is on the same subnet as the PC used to configure this router.

1.4.2.5
Configuring TFTP

Configure the 3Com® TFTP server application when you replace a router in the field and load the router configuration file on a new router during installation.

Prerequisites: Use a dedicated site PC or laptop with 3Com TFTP server application.

Procedure:

1. Select and run the 3Com TFTP application from the Windows Program menu.

   The **3Com 3CServer** window appears.

2. From the TFTP toolbar, click **Setup**.

   The **3CServer Configuration** dialog box appears.

3. Select the **TFTP Configuration** tab.

   The **TFTP Configuration** tab appears.

4. Verify that the router configuration is present on the laptop computer, and that you know its location.
5. Select the router configuration file directory. In the **TFTP Configuration** tab, click **Browse Directories**, select the directory containing the router configuration files. Click **OK**.

1.4.2.6

Transferring the Router Configuration File

Transfer the router configuration file to the replacement router when you replace a router in the field and load the router configuration file on a new router during installation.

Prerequisites: Obtain:

- Appropriate router configuration files
- PC with a terminal emulation program

Procedure:

1. Return to the terminal emulator program. At the `EnterpriseOS#` prompt, type the following commands, and press ENTER after each command:

   ```
   copy 20.0.0.1:<.cfg filename> a:/primary/boot.cfg
   ```

   ```
   copy 20.0.0.1:<.cfg filename> a:/primary/<conf_file.cfg>
   ```

   NOTICE:

   - ***<.cfg filename>*** is the name of the router configuration file specific to the router you are replacing. For example, the configuration file for core router 1 in zone 1 is **z001core01.cfg**.
   - ***<conf_file.cfg>*** is any additional configuration file you are using on the router. For example: acl.cfg or StaticRP.cfg. See Configuration Files – S6000 on page 36 or Configuration Files – S2500 on page 75 for a list of the configuration files required for each router, by network position. You must enter one copy command for each configuration file on the router. For example, if the router requires acl.cfg and StaticRP.cfg files in addition to the boot.cfg file, you would enter:

   ```
   copy 20.0.0.1:<.cfg filename> a:/primary/boot.cfg
   ```

   ```
   copy 20.0.0.1:<.cfg filename> a:/primary/acl.cfg
   ```

   ```
   copy 20.0.0.1:<.cfg filename> a:/primary/StaticRP.cfg
   ```

   The configuration files are transferred to the router, renamed as boot.cfg, acl.cfg and StaticRP.cfg (if used) respectively, and the `EnterpriseOS#` prompt reappears. The router now has the correct identity for the configuration.

2. Verify that the account password is set to the same value as the router.
3. Reboot the router to verify that the correct configuration files were loaded:

a Return to the terminal program.

b At the `EnterpriseOS#` prompt, type **`rb`** (ReBoot). Press Enter.

The router reboots and processes the configuration files. Once complete, `System Initialized and Running` is displayed.

1.4.2.7 Verifying the New Configuration

When you replace a router in the field and load a router configuration file on a new router, reboot the router is rebooted and run the new configuration.

Prerequisites: Use a PC with a terminal emulation program.

Procedure:

1. After `System Initialized and Running` is displayed, log on to the router.
2. At the prompt, type `cd`. Press Enter.
3. At the `EnterpriseOS#` prompt, type `cat boot.cfg`. Press Enter.
4. Compare the Timestamp and Config Summary sections with the original file on the PC.
5. Type **`q`** to quit the display of the boot.cfg file. Press Enter.
6. Follow step 3 to step 5 for the rest of the configuration files for your router.

   The router prompt now displays the system name of the router, rather than `EnterpriseOS#` and the information in the configuration files matches the original files.

7. Power down the router, disconnect the TFTP computer, and connect all system communication cables to the router. Power on the router.

1.4.2.8 Completing the Configuration

Perform certain steps to complete the process of configuring the routers.

Prerequisites: If appropriate, for the systems with link encryption or protocol authentication obtain:

- Pre-Shared Keys (PSKs)
- OSPF/PIM keys or OSPF-BGP keys
- SSH key

When and where to use: Follow this procedure if you replace a router in the field and wish to load a router configuration file on a new router during installation.

Procedure:

1. Power up the router.

   The router reboots using the configuration files you loaded (such as, boot.cfg, acl.cfg, and StaticRP.cfg). The IP address you assigned to the router is replaced with the IP address specific to that router in your system.

2. On systems with MAC port locking, disable the locking on the LAN switch, and then re-enable the locking on the switch with the MAC address of the new router. For instructions on how to disable and enable MAC port locking, refer to the *MAC Port Lockdown* manual.

3. On systems with link encryption, enter the correct pre-shared keys (PSKs) for the new router so that it can be authenticated by its encryption peer. For instructions, refer to the *Link Encryption and Authentication* manual.
4. On systems that require SSH, generate a key for the new router to enable the SSH. For instructions, refer to the *Securing Protocols with SSH* manual.
5. For the centralized authentication feature, the RADIUS authentication sources are already set up in router configuration files by Motorola Solutions. The only RADIUS configuration you need to perform on Motorola Solutions routers is to enter the secret key that matches the “shared secret” for this RADIUS client on the RADIUS server. For instructions, see the *Authentication Services* manual.
6. On systems with SNMP Version 3 enabled, enable SNMPv3 passphrases. For instructions, refer to the *SNMPv3* manual.
7. On systems with protocol authentication, enter the correct OSPF/ PIM or OSPF/BGP keys for the new router so that it can authenticate with its authentication neighbor/peer. For instructions, refer to the *Link Encryption and Authentication* manual.
8. Discover the router in the UNC (if the UNC application is present in the system), refer to the *Unified Network Configurator* manual.
9. Upload the device configuration and hardware information from the router to the UNC. Refer to the “Scheduling the Pull of Device Configurations” section in the *Unified Network Configurator* manual.

Postrequisites: Verify that the router is operating properly.

NOTICE:
Routers are optimized at the factory. No additional optimization procedures are required for the routers.

For routers that are not managed by UNC, store configuration and hardware information from the router locally. Files must be backed up locally as the border router and peripheral network routers exist outside the Motorola Solutions RNI and are not configured or managed by the UNC application.

For routers that are managed by UNC, print out all the router configurations in your system from the UNC and store them in a secure location. If any router upgrades are made, print out the new configurations and replace those routers' records in your records. This provides specific address information for the individual routers. See the *Unified Network Configurator* manual or online help for more information.

For security purposes, all default passwords have to be changed prior to operational use. Those include both 'root' and 'admin' user passwords.

1.4.3

Updating Access Control List Files to Support System Expansions

System expansions require that you update the router access control list (ACL) files (`acl.cfg`) in different scenarios.
These scenarios are:

- Console site expansion – When you add a console site to a trusted group, you must update the `acl.cfg` file for all routers in the trusted group.
- Zone core expansion – When you add a zone core, you must update the `acl.cfg` file for all routers.

Prior to the ASTRO® 25 7.13 system release, the ACL update procedure involved copying the new `acl.cfg` file to the routers and rebooting the routers. The ASTRO®25 7.13 system release introduces the `antiacl.cfg` file, a file that completely removes the current `acl.cfg` settings from a router. By copying the `antiacl.cfg` file and the new `acl.cfg` file to a router, you can update the current ACL/firewall settings without a reboot. You can perform the update procedure manually and automatically.

When and where to use: Update the ACL files in one of the following ways:

- Automatically, in the UNC (M core, or L core systems). For more information, see Automatically Updating Access Control List Files on page 42.

  NOTICE: Downtime cannot be avoided for L1 and M1 systems.

- Manually, using the router command line (K core systems). For more information, see Manually Updating Access Control List Files on page 43.

The following basic process steps are common for manual and automatic ACL updates.

NOTICE: The ACL file distribution and file activation can be implemented as two separate processes and executed at different times.

Process:

1. Distribute the antiacl.cfg and new `acl.cfg` files to the routers.
2. Activate the antiacl.cfg and new `acl.cfg` files.
3. Delete the antiacl.cfg file.
4. For a console site expansion, reboot the core router or routers. For a zone core expansion, reboot the exit router or routers.

   NOTICE: For systems that are redundant in the core, you must reboot both routers in the core or exit router pair. The gateway router does not require a reboot.

Related Links

Automatically Updating Access Control List Files on page 42
Manually Updating Access Control List Files on page 43

1.4.3.1 Automatically Updating Access Control List Files

You can use Unified Network Configurator (UNC) to automatically update Access Control List (ACL) files. You update the files without rebooting the router.

Prerequisites:
Familiarize yourself with the overview information. See Updating Access Control List Files to Support System Expansions on page 41.

Obtain the `antiacl.cfg` and new `acl.cfg` files, from your Motorola Solutions field representative.

When and where to use: Perform this process to support console site expansion or zone core expansions for ASTRO® 25 systems that employ the M core or L core zone cores.

Process:

1. Load the antiacl.cfg and new `acl.cfg` files to the UNC workspace. See the *Unified Network Configurator* manual for information about uploading the configurations for transport devices in the UNC Wizard.
2. Distribute the antiacl.cfg and new `acl.cfg` files to the impacted routers using UNC. Refer to the *Unified Network Configurator* manual for information about distributing configurations for transport devices by using the UNC Wizard.

   NOTICE: You can schedule many distributions of the configuration files. However, when you schedule a very large number of distributions, you may delay other UNC operations.

3. Clear old ACL and activate new ACL files using the UNC Save Command. Refer to the *Unified Network Configurator* manual for information about activating new ACL files.
4. Check the Activation Status of the ACL file. See the *Unified Network Configurator* manual for information about accessing and executing existing saved commands.

Return to Process

Updating Access Control List Files to Support System Expansions on page 41

Related Links

Manually Updating Access Control List Files on page 43

1.4.3.2 Manually Updating Access Control List Files

You can use Unified Network Configurator (UNC) to manually update Access Control List (ACL) files. You update the files without rebooting the router.

Prerequisites:
Familiarize yourself with the overview information. See Updating Access Control List Files to Support System Expansions on page 41.

Obtain the `antiacl.cfg` and new `acl.cfg` files from your Motorola Solutions field representative.

When and where to use: Perform this process on each of the impacted routers to support Console Site Expansion or Zone Core Expansions for ASTRO®25 systems that employ the K core.

Procedure:

1. Use TFTP (non-secure) or PuTTY secure copy protocol (SCP) (secure) to transfer `antiacl.cfg` and `acl.cfg` files to the impacted routers.

   See Transferring the Router Configuration File on page 39.
2. Establish a Telnet (non-secure) or SSH (secure) connection to the router.
3. Activate the antiacl.cfg file. From the router command line, enter:

   ```
   cd
   ```

   ```
   lc antiacl.cfg ie
   ```
4. Check the status of the antiacl.cfg file activation. From the router command line, enter:

   ```
   cat config.log | grep -i error
   ```
5. Activate the new `acl.cfg` file. From the router command line, enter:

   ```
   cd
   ```

   ```
   lc acl.cfg ie
   ```
6. Check the status of the `acl.cfg` file activation by repeating step 4.
7. Delete the `antiacl.cfg` file. From the router command line, enter:

   ```
   rf antiacl.cfg
   ```
8. Perform one of the following actions:
   - For a console site expansion, reboot the core router or routers.
   - For a zone core expansion, reboot the exit router or routers.

Return to Process

Updating Access Control List Files to Support System Expansions on page 41

Related Links

Automatically Updating Access Control List Files on page 42

1.4.4 Router Configuration in the Unified Network Configurator

The Unified Network Configurator (UNC) resides on the User Configuration Server (UCS). You use UNC to perform various actions.

Use UNC to:

- Group the routers to perform the following tasks on more than one router at a time, including:
  - Backing up and restoring routers.
  - Rebooting one or more routers.
- Maintain router configuration and software files, view router information, and launch telnet sessions.
- Prepare the router for management and to configure managed routers. Refer to the *Unified Network Configurator* manual for the following procedures:
  - Preparing the router for management, see the “Configuration Management” section.
  - Restoring a previous router configuration, see the “Rolling Back to a Previous Version” section.
  - Changing a current router configuration and send it to the router, see the “Device Update with a Download of Configuration Changes” section.

NOTICE: This topic does not apply to the Border Router or Peripheral Network Routers.

1.4.5 Backing up the Router Configuration

You can create a backup of the router’s running configuration files and execution image by copying the contents of the router’s primary directory either to the router’s secondary directory or to a TFTP server. This backup includes the Motorola Solutions-provided configuration files as well as other manually-entered configuration, such as pre-shared keys. In the event that the contents of the router’s primary directory are corrupted, you can restore the configuration files and execution image from the backup.

Use these procedures to create backups which you can use to recover the router configuration in the event of a failure.

NOTICE: The backups created by these procedures are specific to the physical motherboard from which the primary directory contents are copied. In other words, these backups work only if the motherboard from which you copied the configuration files and execution image is installed in the device you are restoring. You cannot use the backups created by these procedures if you are swapping one device for another or if you are replacing a motherboard.

1.4.5.1 Creating a Local Backup

To create a local backup, use the following procedure to copy the contents of the router’s primary directory to the router’s secondary directory.

Prerequisites: PC with a terminal emulation program.

Procedure:

1 At the `EnterpriseOS#` prompt, enter the following command to clean up the previous backup:

```
RF a:/secondar/*.*
```

2 Enter the following command to make a copy of the current running configuration and execution image:

```
COPY a:/primary/*.* a:/secondar
```

3 Check if there are any subdirectories of the **a:/primary** directory. If so, repeat steps 1 and 2 above for each subdirectory, replacing `a:/primary/` with the path to the subdirectory in the `COPY a:/primary/*.* a:/secondar` command.

4 To subsequently restore the router configuration from the backup in the secondary directory in the event that the contents of the primary directory have become corrupted, follow these steps:

   a From the `EnterpriseOS#` prompt, enter `SF 7` to open the **SysconF** command Boot Sources menu.

   b Enter 3 to direct the router to boot from the secondary directory.

   c Reboot the router.

1.4.5.2 Backing Up to a TFTP Server

To back up the contents of the router's primary directory to a TFTP server, use the following procedure.

Prerequisites: Dedicated site PC or laptop with TFTP server application.

Procedure:

1 Connect a straight-through Ethernet cable between the router and a hub or switch port that is in the same subnet as the TFTP server.

2 At the `EnterpriseOS#` prompt, enter the following commands to configure the router to access the TFTP server:

```
SETDefault !3 -IP NETaddr = <IP address> [<network mask>]
```

Where ***<IP address>*** is the IP address you want to assign to the router's Ethernet port and ***<network mask>*** is the subnet mask.

```
SETDefault !3 -PAth CONTrol = Enable
```

```
SETDefault !3 -POrt CONTrol = Enable
```

```
ADD -IP ROUte <IP address> <mask> <gateway> <metric>
```

Where ***<IP address>*** is the subnet address for the TFTP server, ***<mask>*** is the subnet mask, ***<gateway>*** is the gateway IP address, and ***<metric>*** represents the number of hops required for a packet to reach its destination.

Step example:

```
SETDefault !3 -IP NETaddr = 10.79.130.128 255.255.255.0
```

```
SETDefault !3 -PAth CONTrol = Enable
```

```
SETDefault !3 -POrt CONTrol = Enable
```

```
ADD -IP ROUte 10.79.0.0 255.255.0.0 10.79.130.1 0
```

3 Enter the following command to generate a list of files in the router's primary directory: `DF a:/primary`

4 Use the list of file names generated in step 3 to create a list of copy commands, one command for each file name, and enter them one at a time until all the files in the list have been copied.

Step example:

For example, if the list returned by the DF command consists of a boot.ppc file and a boot.cfg file, enter the following commands to copy the files to a directory named backup1 on the TFTP server with IP address 10.79.0.2:

```
copy a:/primary/boot.ppc 10.79.0.2:/backup1
```

```
copy a:/primary/boot.cfg 10.79.0.2:/backup1
```

NOTICE: If the list returned by the DF command includes other files in addition to the boot.ppc and the boot.cfg files, then you must enter additional copy commands (one command for each file), substituting the filename(s) of the additional files for boot.ppc or boot.cfg in the examples above.

5 To subsequently restore the router configuration files and execution image from the backup on the TFTP server in the event that the contents of the router’s primary directory have become corrupted, follow these steps:

a From the `EnterpriseOS#` prompt, enter a copy command for each file in the backup directory. For example, if backup directory backup1 on the TFTP server with IP address 10.79.0.2 includes a boot.ppc file and a boot.cfg file, enter the following commands:

```
copy 10.79.0.2:/backup1/boot.ppc a:/primary
```

```
copy 10.79.0.2:/backup1/boot.cfg a:/primary
```

NOTICE: If the backup directory includes other files in addition to the boot.ppc and the boot.cfg files, then you must enter additional copy commands (one command for each file), substituting the filename(s) of the additional files for boot.ppc or boot.cfg in the examples above.

b Reboot the router.

1.4.6 Router Discovery by the Use of UEM

Once the router is discovered and configured in the Unified Network Configurator (UNC), the router must be discovered in the Unified Event Manager (UEM) for fault management. The active router is discovered as part of the subnet discovery. Refer to the *Unified Event Manager* manual for more information on this procedure.

NOTICE: The router must be discovered in the UEM for traps and events to appear in the UEM.

1.5 S6000 Operation

Perform certain tasks after installing and using the router on your system.

1.5.1 Router Administration

You can administer routers in different ways.

Nearly all the necessary router administration can be performed in the Unified Network Configurator (UNC). For the information to locally set up the basic router configuration, refer to the *Unified Network Configurator* manual.

However, when the router does not have an established connection with the master site LAN or is not managed by UNC, you can administer basic router information, such as its IP address, gateway address and other configuration parameters in two ways:

- Through the terminal server menus

- Directly through a connection to the console port on the router

⚠ **CAUTION:** Do not tamper with the factory configuration settings for these devices. This includes software configuration, firmware release, password, and physical connections. Motorola Solutions has configured and connected these devices to meet very specific performance requirements. Tampering with these devices may result in unpredictable system performance or catastrophic failure.

For information on how to connect to a router through a terminal server emulator and configure the router IP address, see Configuring the IP Address and Workstation Connections on page 37.

1.5.2 Power Up – S6000 LEDs Status

Powering up the router takes a few seconds and when the process is successfully completed, the LEDs on the front panel display differently.

Table 7: LED Status after Successful Power Up

LED	Status
LAN	
100 Mbps	ON if connected to 100 Mbps link, or OFF if connected to 10 Mbps link
Link	ON
Active	OFF or blinking
Fault	OFF
UltraWAN CSU/DSU	
Carrier	ON
Alarm	OFF
Lpbk	OFF
SYSTEM	
Status	All OFF
Fwd	OFF or blinking
Power/Fault	Green
Run	ON
Load	OFF
Test	OFF
FlexWAN	
Link	ON
Active	ON or OFF
Fault	OFF
12-port T1/E1	
	Green (for active peer) Yellow (for inactive peer)

NOTICE: During power up, the UltraWAN CSU/DSU LEDs periodically flash ON and OFF. When the power up process is complete, these LEDs remain OFF. When the UltraWAN CSU/DSU interfaces are configured and the interfaces are operational, these LEDs remain ON. Depending on the I/O modules installed in the S6000 router, some of the status information may not apply to specific configurations.

1.6 S6000 Maintenance

This section describes periodic maintenance procedures relating to the router.

1.6.1 Maintaining Routers

The router does not contain serviceable parts that require maintenance or calibration. Maintaining requires only basic procedures.

Follow the basic rules for the router maintenance:

- Use a clean, lint-free cloth or a soft brush for exterior cleaning.
- Ensure that the ventilation ports are kept clean at all times.
- Monitor the router LEDs periodically to ensure that the router is operating properly.

NOTICE: It is also advisable to do periodic interior cleaning by using a low-suction vacuum cleaner.

1.7 S6000 Troubleshooting

This section provides fault management and troubleshooting information relating to the routers.

1.7.1 Troubleshooting the Router

The following resources are available for troubleshooting problems with the managed routers:

- Unified Network Configurator (UNC)
- Unified Event Manager (UEM)
- Local router administration (performing the task on the router through a direct connection to the console port on the router)

NOTICE: The Border Router and Peripheral Network Routers are not configured or managed by UNC or UEM. Actions must be performed locally as these routers exist outside the Motorola Solutions Radio Network Infrastructure (RNI).

See the *Unified Event Manager Online Help* for details on the alarms for the routers.

1.7.1.1 Troubleshooting General Connectivity Problems

Troubleshoot general connectivity problems by checking the alarms and physical connections or reloading the configuration files.

Prerequisites: Install and configure the router.

When and where to use: Use the following steps to troubleshoot the router's connectivity problems related to the LAN connection.

NOTICE: The Border Router and Peripheral Network Router do not support the UNC/UEM procedures. You can perform the same tasks locally using the router administration menus.

Procedure:

1 Perform the following actions:

- In the Unified Event Manager (UEM), check the conditions and alarms for the router.
- In the Unified Network Configurator (UNC), check the router configuration and router log information.
- Verify that the IP address, MAC address, and other configuration settings are correct.

2 Using UEM, check the alarms for other critical network devices on the LAN. Also, verify the configuration of the LAN switch.

3 Check the physical connection to the LAN port on the router. Verify that the cabling is properly connected and in good condition.

4 Try to reboot the router through the UNC or cycle power to the router. See the *Unified Network Configurator* manual for more information.

5 If the router fails to establish a connection, power down the router, and test the Ethernet cable for continuity, attenuation, and excessive crosstalk. Replace the cable if necessary.

6 If the connection still fails, try to reload the EOS software and configuration files to the router locally or through the Unified Network Configurator (UNC). See the *Unified Network Configurator* manual for instructions.

7 If the router still fails to operate properly, replace the router.

1.7.1.2 Troubleshooting General Performance Problems on the LAN

Troubleshoot LAN performance problems of the routers by using the Unified Event Manager (UEM), Historical Reports, Performance Reports, InfoVista, or checking the physical connections.

Prerequisites: Install and configure the router.

When and where to use: Use the following steps to troubleshoot the router's performance problems on the LAN.

NOTICE: The Border Router and Peripheral Network Router do not support the UNC/UEM procedures. You can perform the same tasks locally using the router administration menus.

Procedure:

1 In the UEM, check the condition of the LAN switch and all affected devices and links. Verify that all the routers are operational.

2 Using Historical Reports and Performance Reports, check the overall loading of calls and activities on the LAN. Verify that the loading is within the maximum loading specifications for the system.

3 Using InfoVista, generate performance and traffic reports for the routers. Look for anomalies, heavy volumes of traffic, or high CPU utilization, or other device resources.

   NOTICE: InfoVista is an option for ASTRO® 25 systems. The Border Router and Peripheral Network Router do not support InfoVista.

4 Run ping, traceroute, pathping commands, and loopback testing across any troubled links or between any suspected devices.

5 Verify that the address tables, subnet masks, and default gateways are set correctly in the router and other networked devices.

6 Physically verify that the LAN switch is operating properly. Check the LEDs and physical connections, and verify that all cabling conforms to the standard. Check for sharp bends in cabling and cable length not adhering to the specification (such as 100 meters for 10Base-T).

7 Check the troubled cabling for noise, attenuation, continuity, and crosstalk. Verify that the communication cabling is routed apart from all power cabling and power sources. Verify that the cabling is also clear from any test equipment that may cause interference.

8 As applicable, verify that any service provider connections are providing the appropriate throughput for the system.

9 Identify the bottleneck points in the system. Check and reload device configurations as necessary, or replace any suspected switching or routing devices that may not be performing to specification.

10 Revise the configurations, services, and permissions for the subscribers as necessary.

11 Purchase additional equipment to handle the additional load of traffic (more routers or sites). Contact Motorola Solutions for assistance.

1.7.2 LED Indicators – S6000

The indication of each LED informs the user about the S6000 router status.

LAN LEDs
Indicate the conditions and activity for each of the Ethernet ports connected to the LAN.

UltraWAN LEDs
Indicate the conditions and activity for each UltraWAN port on the router.

FlexWAN LEDs
Indicate the conditions and activity for each FlexWAN port on the router.

System LEDs
Indicate the overall condition of the router system, including its operating status, power conditions, and fault conditions.

NOTICE: For more information on the LEDs statuses, refer to the troubleshooting sections in this manual.

Table 8: S6000 Router LED Indicators

LED Type	LED	Description
LAN	100 Mbs	Illuminates **Green** when 100Base-TX Ethernet is in use.
	Link	Illuminates **Green** when the Ethernet link is established.
	Active	Flickers **Green** when the Ethernet port is receiving or transmitting packets.
	Fault	Illuminates **Amber** when an error is detected or the self-test has failed.
UltraWAN	Carrier	Illuminates **Green** when the port is synchronized with the T1 carrier.
	Alarm	Illuminates **Amber** when an alarm condition is being reported for the frame relay interface.
	Loopback (Lpbk)	Illuminates **Amber** when a connector-level loopback is in progress.
FlexWAN	Link	Illuminates **Green** when the link is established.

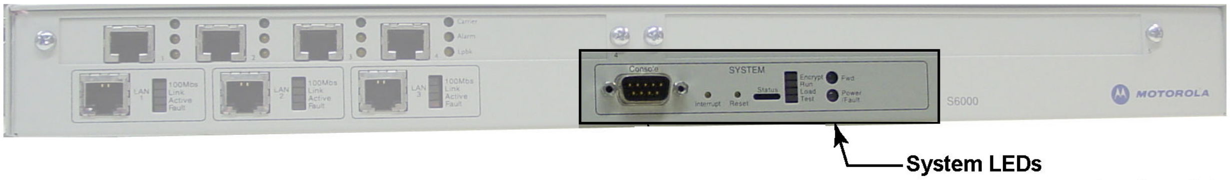
LED Type	LED	Description
	Active	Flickers **Green** when there is activity on the port.
	Fault	**OFF** in normal operation. Illuminates **Amber** when an error is detected or the self-test has failed.
System	Encrypt	The Encrypt LED is not used in this release.
	Run	Illuminates **Green** when the router has successfully loaded, all start-up diagnostics have passed, and is operating normally.
	Load	**OFF** in normal operation. Flickers **Amber** during startup to indicate the system is loading software. Illuminates **Amber** when there is a load problem.
	Test	**OFF** in normal operation. Illuminates **Amber** during startup to indicate the system is running self-tests.
	Status	Provides additional status for the Run, Load, and Test LEDs. Four status LEDs show a code indicating specific types of loading failures. For the codes shown, zero (0) represents an extinguished LED and one (1) represents an illuminated LED.
	Forward (Fwd)	Flickers **Green** each time a packet is forwarded between the two Ethernet ports.
	Power/Fault	Illuminates **Green** when the unit has power. Illuminates **Amber** if there is a problem with power. When unlit, power to the unit is **OFF**.

1.7.3
System LEDs Troubleshooting – S6000

The indication of each LED informs the user about the S6000 router status. The System LEDs indicate the overall condition of the router system, including its operating status, power conditions, and fault conditions.

When a router failure occurs, the four Status LEDs can also indicate a failure code that defines the particular problem. The System LEDs are located near the console port on the front of the router. The four Status LEDs show a code indicating specific types of loading failures. For the codes shown, zero (0) represents an extinguished LED and one (1) represents an illuminated LED.

Figure 6: System LEDs



RouterSystemleds

NOTICE: The Border Router and Peripheral Network Routers are not configured or managed by the Unified Network Configurator (UNC) or Unified Event Manager (UEM) applications. Actions must be performed locally as these routers exist outside the Motorola Solutions Radio Network Infrastructure (RNI). In the following table, if the step indicates using UEM or UNC, perform the task locally on the router through a direct connection to the console port on the router.

Table 9: System LEDs

LED	Indication	Status and Troubleshooting Action
Encrypt	N/A	The Encrypt LED is not used in this release.
Run	Green	Indicates the router has successfully loaded, all startup diagnostics have passed, and the router is operating normally. No action is necessary.
	OFF	The router is not powered or is not running properly. **1** Use UEM to check the conditions and alarms for the router. **2** Verify that the Power/Fault LED is solid Green and the Load LED is OFF. • If the Power/Fault LED is extinguished, there can be a problem with the power input. • If the Load LED is illuminated, then there can be a loading problem. Follow the troubleshooting steps for these other LEDs for more information.
Load	OFF	Router is loaded and operating normally. No action is necessary.
	Flickering Amber	Router is initializing. No action necessary.
	Amber	The router is experiencing a loading problem. This is typically accompanied by a solid Amber indication by the Power/Fault LED. The Status LEDs indicate the specific type of loading problem. See the Status LED troubleshooting steps for more information. **1** Using UEM or applicable fault management application, check the conditions and alarms for the router. **2** Cycle power to the router. **3** If the router continues to iterate through the boot process without finally moving into the run mode, contact the Motorola Solutions Support Center (SSC) for assistance.
Test	OFF	The router is operating normally. No action is necessary.
	Amber	The router is performing self tests. No action is necessary.
Status	0001	The router file system is empty. Try reloading the EOS software and configuration files through the UNC. Refer to the *Unified Network Configurator* manual for instructions.
	0010	A read-only memory corruption is detected. Cycle power to the router and try reloading the EOS software and configuration files locally or through the UNC.
	0011	The software image file is deleted or the boot source and image names do not match. If the Test LED is also illuminated, the router is indicating an EEPROM checksum error. **1** Cycle power to the router and see if the condition is cleared. **2** If the condition does not clear, try reloading the EOS software and configuration locally or through the UNC.

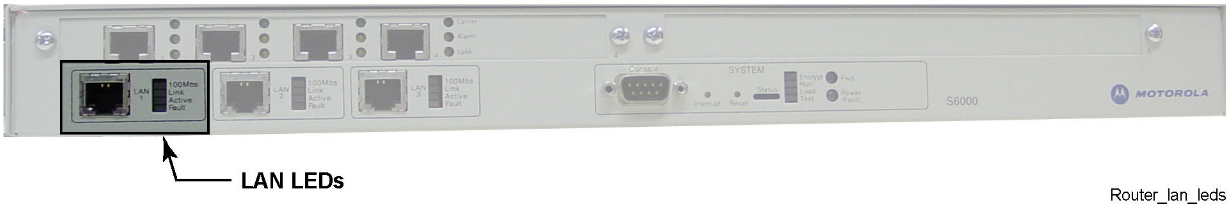
LED	Indication	Status and Troubleshooting Action
		3 If the problem is not resolved, replace the router or contact Motorola Solutions Support Center (SSC) for assistance.
	0101	The file size is larger than available memory. **1** Cycle power to the router and see if the condition is cleared. **2** If the condition does not clear, try reloading the EOS software and configuration files locally or through the UNC. **3** If the problem is not resolved, replace the router or contact Motorola Solutions Support Center (SSC) for assistance.
	0100	A file read or decompression error has been detected. Cycle power to the router and try reloading the EOS software and configuration files locally or through the UNC.
	0110	A file checksum error has been detected. Cycle power to the router and try reloading the EOS software and configuration files locally or through the UNC.
	0111	An unspecified fatal error has occurred. **1** Cycle power to the router and try reloading the EOS software and configuration files locally or through the UNC. **2** If the router does not boot properly, use UEM or the applicable fault management application to check the alarms for the router. **3** If the router still fails to operate properly, replace the router.
Forward (Fwd)	Flickering Green	Packets are being forwarded between the two Ethernet ports. No action is necessary.
Power/ Fault	Green	The router is properly powered. No action is necessary.
	Amber	The router is reporting a fault condition. Troubleshoot the router according to the Load LED and Status LED troubleshooting instructions above. **1** Check the Load LED and Status LEDs for additional error indications. Use the troubleshooting steps for the Load LED or Status LEDs if they are illuminated. **2** Check the conditions and alarms for the router. Use UEM for managed routers. **3** Try rebooting the router through the UNC for managed routers or cycle power to the router. **4** If the router does not boot properly, try reloading the EOS software and configuration files locally or through the UNC. **5** If the router still does not run properly, replace the router.
	OFF	The router is not powered. **1** Check the conditions and alarms for the router. Use UEM for managed routers. **2** Connect the router to a different power source that is operational. Verify that the power cabling is firmly connected in the rear of the router.

LED	Indication	Status and Troubleshooting Action
		NOTICE: If possible, maintain redundant routers on separate circuits. **3** If the router still does not boot up, replace the router.

1.7.4
LAN LEDs Troubleshooting – S6000

The Local Area Network (LAN) LEDs indicate the fault conditions and activity for each of the Ethernet ports connected to the LAN. The S6000 router features up to three LAN ports. The LAN port has four LEDs.

Figure 7: LAN LEDs



Router_lan_leds

NOTICE: The Border Router and Peripheral Network Routers are not configured or managed by the Unified Network Configurator (UNC) or Unified Event Manager (UEM) applications. Actions must be performed locally as these routers exist outside the Motorola Solutions Radio Network Infrastructure (RNI). In the table below, if the step indicates using UEM or UNC, perform the task locally on the router through a direct connection to the console port on the router.

Table 10: LAN LEDs

LEDs	Indication	Status and Troubleshooting Action
100 Mbs	Green	Indicates when 100Base-TX is in use, when the port is operating with a 100Base-TX connection. No action is necessary.
Link	Green	The Ethernet link is established. No action is necessary.
	OFF	The Ethernet link is not established for some reason. **1** Use UEM to check the conditions and alarms for the router. Then, use UNC to check the router configuration and router log information. Verify that the IP address, MAC address, and other configuration settings are correct. **2** Verify the configuration for the router in the UNC. If applicable, send an enable diagnostic command for the router through UNC. **3** Check the physical connection to the LAN port. Verify that the cable is properly connected and in good condition. Try using a shorting plug connecting pins 1-3, 2-6 to verify port links locally on the device. **4** Try to reboot the router through the UNC or cycle power to the router. **5** If the port fails to establish a connection, power down the router and test the Ethernet cable for continuity, attenuation, and excessive crosstalk. Replace the cable if necessary.

LEDs	Indication	Status and Troubleshooting Action
		6 If the port still fails, try to reload the EOS software and configuration files to the router locally or through the UNC. **7** If the router still fails to operate properly, replace the router.
Active	Flickering Green	Indicates that packet activity is taking place on the LAN and that the Ethernet port is actively receiving or transmitting packets. No action is necessary.
	OFF	No packet activity is detected. If the port should be active, troubleshoot the router as explained for a Link LED failure above.
Fault	OFF	The port is ok. No action is necessary.
	Amber	A fault has been detected or the self test for the port has failed. **1** Using UEM, check the conditions and alarms for the router. Also check the router configuration and router log information in the UNC. **2** Check the physical connection to the LAN port. Verify that the cable is properly connected and in good condition. **3** Try to reboot the router through the UNC, or cycle power to the router. **4** If the port fails, try to reload the EOS software and configuration files to the router locally or through the UNC. **5** Verify that the port speeds and duplex match between the router and the device it is connected to on the LAN port. **6** If the router still fails to operate properly, replace the router

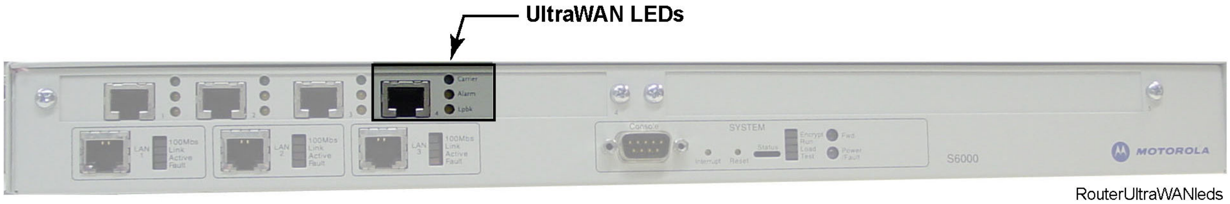
NOTICE: Refer to the *Unified Network Configurator* manual or online help for detailed instructions.

1.7.5

UltraWAN LEDs Troubleshooting – S6000

The UltraWAN LEDs indicate the conditions and activity for each UltraWAN port on the router. The LEDs indicate the T1 carrier condition, loopback mode activity, and any alarms for each port.

Figure 8: UltraWAN LEDs



RouterUltraWANleds

NOTICE: The Border Router and Peripheral Network Routers are not configured or managed by the Unified Network Configurator (UNC) or Unified Event Manager (UEM) applications. Actions must be performed locally as these routers exist outside the Motorola Solutions Radio Network Infrastructure (RNI). In the following table, if the step indicates using UEM or UNC, perform the task locally on the router through a direct connection to the console port on the router.

Table 11: UltraWAN LEDs

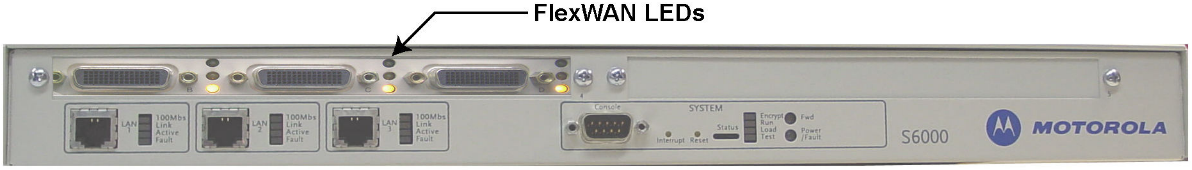
LED	Indication	Status and Troubleshooting Action
Carrier	Green	Indicates the frame synchronization to the T1 carrier. If Green, the port is synchronized with the T1 carrier. No action is necessary.
	OFF	The port is not synchronized with the T1 carrier for some reason. Verify that the port is enabled and a proper connection is made to the port. Check if the Alarm LED is illuminated.
Alarm	OFF	The port is not reporting any alarm conditions. No action is necessary.
	Amber	An alarm condition is being reported for the frame relay interface, such as a Far End Block Error (FEBE), Alarm Indication Signal (AIS), or Remote Alarm Indication (RAI). **1** Using UEM, check the conditions and alarms for the router. Also check the router configuration, router event log, and history of router configuration changes as available in the UNC. **2** Check the conditions and alarms of the far end equipment. **3** Try to reboot the router through the UNC, or cycle power to the router. Refer to the *Unified Network Configurator* manual for more information. **4** If the alarm does not clear, check the physical connection to the affected port. Verify that the cable is properly connected and in good condition. Test local cabling for attenuation, noise, and crosstalk. Replace if necessary. **5** Test the condition of the layer 1 frame relay interfaces, including signal levels, line encoding, clock rates, and bit error rates. **6** Verify that the service provider is supplying the appropriate bandwidth and a sufficiently low bit error rate across the link. **7** Try using an RJ-45 shorting plug connecting pins 1-4, 2-5 to verify port links locally on the device. **8** Verify channel bandwidth and interfaces for a needed crossover connection or straight through. **9** If the port still fails, try to reload the EOS software and configuration files to the router locally. **10** If the router still fails to operate properly, replace the router.
Loopback (Lpbk)	OFF	No loopback in progress. No action is necessary.
	Amber	A connector-level loopback is in progress. If loopback mode is not desired, close the loopback mode and set the port back to the frame relay mode. Refer to the *Motorola Network Router (MNR) S6000 Hardware User Guide* for specific instructions.

1.7.6 FlexWAN LEDs Troubleshooting – S6000

The FlexWAN LEDs indicate the conditions and activity for each FlexWAN port on the router.

The FlexWAN port is used for the V.35 serial connection to the High-Speed Unit (HSU) card on the channel bank when circuit-based Conventional channels are supported at the site.

Figure 9: FlexWAN LEDs



FlexWAN_LEDs

NOTICE: The Border Router and Peripheral Network Routers are not configured or managed by the Unified Network Configurator (UNC) or Unified Event Manager (UEM) applications. Actions must be performed locally as these routers exist outside the Motorola Solutions Radio Network Infrastructure (RNI). In the table below, if the step indicates using UEM or UNC, perform the task locally on the router through a direct connection to the console port on the router.

Table 12: FlexWAN LEDs

LED	Indication	Status and Troubleshooting Action
Link	Green	The link is established. No action necessary.
	OFF	The link is not established for some reason. **1** Using UEM, check the conditions and alarms for the router. Also check the router configuration and router log information in UNC. Lastly, check the alarms and configuration for the device on the other end of the link. **2** Verify the configuration for the router in the UNC. If applicable, send an enable diagnostic command for the router through UEM. **3** Check the physical connection to the port. Verify that the cable is properly connected and in good condition. **4** Try to reboot the router through UNC, or cycle power to the router. **5** (For remote routers) Put the remote device into DTE loopback to verify that the FlexWAN connection comes up back to the router. **6** If the port fails to establish a connection, power down the router and test the cable for problems, as possible. Replace the cable if necessary. **7** If the port still fails, try to reload the EOS and configuration files to the router through UNC. **8** If the router still fails to operate properly, replace the router.
Active	Flickering Green	Indicates that activity is detected on the port. The port is sending and receiving traffic normally. No action necessary.
	OFF	No activity is detected. If the port should be active, troubleshoot the router as explained for a Link LED failure above.
Fault	OFF	The port is okay. No action necessary.
	Amber	A fault has been detected or the self-test for the port has failed. **1** Using UEM, check the conditions and alarms for the router. Also check the router configuration and router log information in the UNC. **2** Check the physical connection to the port. Verify that the cable is properly connected and in good condition. Replace if necessary.

LED	Indication	Status and Troubleshooting Action
		3 Try to reboot the router through UNC, or cycle power to the router.
		4 If the port still fails, try to reload the EOS and configuration files to the router through UNC. Refer to the *Unified Network Configurator* manual for instructions.
		5 (For remote routers) Verify that the speed, duplex, flow controls, connector type, and clocking are all correct between the router and the connected device. Try putting the remote device into a DTE loopback to verify link connectivity.
		6 If the router still fails to operate properly, replace the router.

NOTICE: Refer to the *Unified Network Configurator* manual or online help for detailed instructions.

1.7.7 Troubleshooting Routers in the Unified Network Configurator (UNC)

The Unified Network Configurator (UNC) uses VoyenceControl to configure and monitor the status of the routers. Using the router management function, the configurations are viewed, created, and modified using templates. For the step-by-step procedures, refer to the “UNC Operation” chapter of the *Unified Network Configurator* manual.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.
This topic does not apply to unmanaged routers – the Border Router and Peripheral Network Routers or if the system is supported by a K core.

1.7.8 Troubleshooting Traps in the Unified Event Manager (UEM)

Alarms and traps generated by routers are sent to the Unified Event Manager (UEM) server located in the same zone as the site in which the router is located. The remote site router must be discovered in the UEM application using subnet discovery before traps are visible in UEM.

Router faults, events, alarms, and link up/down status are reported in the UEM application. For additional information on subnet discovery as well as a list of router alarms and traps and their definitions, refer to the *Unified Event Manager Online Help*.

NOTICE: This topic does not apply to unmanaged routers – the Border Router and Peripheral Network Routers.

1.8 S6000 FRU/FRE Procedures

This section lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs), and includes replacement procedures applicable to the routers.

1.8.1 Tools and Equipment Required for Router Replacement

Specific tools and equipment are required during the router replacement at the site.

Take the following items to the site when replacing the routers:

- Electrostatic Discharge (ESD) strap (Motorola Solutions part number RSX4015A, or equivalent)

- Laptop PC with a 3Com Trivial File Transfer Protocol (TFTP) server software and a terminal emulation program such as HyperTerminal or ProComm+ installed
- Ethernet crossover cable
- DB9 null modem cable
- Crosstip and slotted screwdrivers
- Set of TORX drivers

1.8.2
Shipping Carton Content

When you receive the router, verify that the carton includes the following items:

- Router configured with I/O modules based on router function
- Power cable
- Rack-mount kit
- EOS Software and User Documentation media device

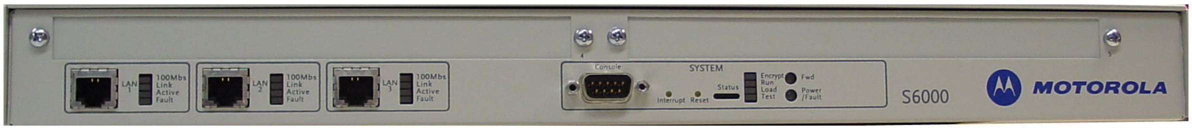
  NOTICE: The software is pre-installed in the flash memory drive of the router and automatically loads when you turn on the power. Software provided on a media device is for software recovery purpose only.

- Release notes
- License agreement

1.8.3
Field Replaceable Entity – S6000

In case of replacement, use a part numbers list for ordering the base S6000 router field replaceable entity (FRE).

Figure 10: S6000 Field Replaceable Entity with no I/O Modules Installed



S6000_router_front

Table 13: S6000 Field Replaceable Entity

Part Number	Component Type	Description
ST6000	S6000 router. No I/O modules required.	The S6000 base router provides three built-in Ethernet ports, LAN 1, LAN 2, and LAN 3. The LAN ports provide connection to Ethernet LANs using either 10Base-T or 100Base-TX Ethernet.

1.8.4 Replacing a Router – S6000

Replacing a router consists of removing the existing router, installing, and then configuring the replacement router.

Prerequisites: Verify that you have access to the appropriate router configuration files for the router you are replacing. You can find the files on the media device containing the electronic version of the system-specific configuration documentation provided by Motorola Solutions. If you do not have access to the media device, contact your system administrator.
Wear an Electrostatic Discharge (ESD) strap and connect its cable to a verified good ground.

Go to Configuration Prerequisites on page 35 for all necessary prerequisites.

CAUTION: Wear the Electrostatic Discharge (ESD) strap throughout the whole procedure to prevent ESD damage to any components.

NOTICE: If redundant site links are supported, powering down an active site router causes the redundant site router to route the full load of traffic for the site, and communication is not affected. However, if redundant site links are not supported, powering down the site router causes the repeater site to enter site trunking mode until the router is operational again.

IMPORTANT: Pull configuration and hardware information from the router into the Unified Network Configurator (UNC) by performing a “Pull All” procedure” from the UNC. Refer to “Scheduling the Pull of Device Configurations” procedure, in the *Unified Network Configurator* manual.

A “Pull All” is not possible if communication is severed between the router and UNC, if the router is not managed by UNC, or if the system is supported by a K core. If any of these scenarios exist, perform any one of the following:

- Use the last known good configuration files from the UNC
- Extract the configuration files from the router directly
- Use the configuration files provided by Motorola Solutions when your system was commissioned. Typically, configuration files are provided on a media device as part of the Electronic Build Book.

No matter what the source of the Configuration files is, the files themselves need to be copied to the service PC with 3com TFTP software enabled.

NOTICE: If you replace a router as a unit, the replacement router must have the same hardware configuration (that is, the same I/O modules installed in the same I/O module slots).

When and where to use:

IMPORTANT: Power down the router before servicing or replacing any interface modules. Powering down a router causes network services to and from the supported site to be suspended until the router is replaced and brought back into service. Wide area voice traffic and networking services should not be affected, but the traffic capacity may be reduced until the router is brought back into service.

Procedure:

1. (Master Site Routers only) If the S6000 router is a CWR peer, before powering the router down, verify that the router does not have the CWR relay panel active (session). Push all CWR ports on the CWR panel to the alternate, standby router.
2. Power down the existing router by disconnecting the power cable from the router and remove any cables that are installed on the chassis.

   DANGER: Shock hazard: Routers contain dangerous voltages, which can cause electrical shock or damage to equipment. Turn off the router and remove the power cabling when servicing this equipment.

3 Remove the existing router:

   a Label and disconnect all communication cabling from the router.

   b Disconnect the ground cable from the rear of the chassis.

   c Remove the screws securing the router to the rack.

   d Pull out the router through the front of the rack.

4 Remove the mounting brackets from the existing router and install the brackets on the replacement router.

5 Install the replacement router:

   a Install the replacement router in the rack and secure it with the screws that were previously removed.

   b Secure the ground cable to the ground location on the rear of the chassis.

   c Attach all communication cabling to the router.

6 Power up the replacement router by reconnecting the power cable to the router.

7 Configure the router according to the process in Router Configuration on page 35.

   NOTICE: When replacing a router, Completing the Configuration on page 40, step 8, which directs you to discover the router in the UNC, does **NOT** apply. Instead, perform the following steps from the process “Replacing a Device” in the *Unified Network Configurator* manual:

   a For this device, execute the **Clear USM Cache** saved command from the list of saved commands under **System**, **Motorola**, then **SNMPv3**. For instructions on accessing and executing saved commands for a device, see “Accessing and Executing Existing Saved Commands” in the *Unified Network Configurator* manual.

   b Use the test credential quick command to test the credentials. For instructions, see “Executing Quick Commands” in the *Unified Network Configurator* manual.

   c Pull the configuration for the new device. For instructions, see “Pulling the Configuration for a Single Device”in the *Unified Network Configurator* manual.

8 Compare the version of the Enterprise Operating System (EOS) software that is running on the replacement router with the version that was running on the replaced router, by running the Compare function in the hardware history in the UNC. See “Comparing Device Configuration Versions” in the *Unified Network Configurator* manual.

   NOTICE: If the replacement router needs a software update, perform the upgrade. Perform “Operating System and Software Upgrade” as described in the *Unified Network Configurator* manual.

9 Check the version of the firmware if performing a downgrade. If the version is 16.8.0.19 or higher for an NMR, additional steps are necessary. See Performing a Firmware Downgrade on page 250.

10 Check for any differences between the configurations, and determine whether either configuration needs to be corrected.

   - If the previous configuration needs to be restored, then refer to the “Rolling Back to a Previous Version” section in the *Unified Network Configurator* manual.
   - If the current configurations are changed and sent to the router, see the “Device Update with a Download of Configuration Changes” section in the *Unified Network Configurator* manual.

Postrequisites: Verify that the replacement router is operating properly.

1.8.5 Field Replaceable Units – S6000

The base router (model ST6000) is configured with the I/O modules necessary to meet the operating requirements of each functional router. The I/O modules are Field Replaceable Units (FRUs). In case of replacement, use a part numbers list for ordering the FRUs.

The S6000 base router ships with the following:

- Three Ethernet (10Base-T/100Base-TX) ports, named LAN 1, LAN 2, and LAN 3
- A console (serial) port
- Two I/O slots for optional I/O modules

The I/O modules are installed in slots labeled with port numbers 4 and 5. The following table lists the FRU information.

FRUs for S6000 Routers

The following table lists the FRU information.

Table 14: FRUs for S6000 Routers

FRU Module ID	FRU Brief Description	FRU Expanded Description
ST6010	4-port T1/E1 UltraWAN I module	Supports integrated, channelized T1/E1, Channel Service Unit (CSU)/Data Service Unit (DSU). The T1/E1 port is the master site to prime site interface.
ST6017	4-port T1/E1 UltraWAN II module	
ST6011	4-port FlexWAN module	Provides a high-speed multifunction serial interface to V.35, RS-232, RS-449, EIA-530, or X.21 Data Communications Equipment (DCE) or Data Terminal Equipment (DTE) serial devices. The FlexWAN port handles master site to channel bank at a remote site supporting a circuit-based Conventional channel.
ST6013	1-port T3/E3 WAN module	Interfaces to an external CSU/DSU using the connector or directly to a T3 or E3 line using the BNC connector.
ST6015	12-port T1/E1 I (CWR) module	Provides WAN interface support for high-density T1/E1 connections. Used for: • Remote Site Access Router • Cooperative WAN Routing (CWR). To order CWR components, refer to the *Cooperative WAN Routing* manual.
ST6018	12-port T1/E1 II (CWR) module	

NOTICE: The S6000 supports two versions of the UltraWAN module and two versions of the 12-port T1/E1 module. The functionality of the two module versions is the same; however, the UltraWAN II and 12-port T1/E1 II modules (identified by a Roman numeral "II" on the front panel), require Enterprise Operating System (EOS) software version 15.4 or higher.

⚠ **CAUTION:** If you install an UltraWAN II or a 12-port T1/E1 II module in an S6000 running a version of EOS software lower than the required version, the router reboots continuously.
For information on Ethernet connectivity between the sites and zones, refer to the *Flexible Site and InterZone Links* manual.

Table 15: FRUs by Router Usage

S6000 Router		ST6010/ ST6017 UltraWAN I/II	ST6011 FlexWAN	ST6013 T3/E3	ST6015/ ST6018 12-port T1/E1 I/II
Border Router		X	X	N/A	N/A
Peripheral Network Router		X	X	N/A	N/A
Master Site Routers:	Core Router (CWR)	N/A	N/A	N/A	X
	Exit Router (CWR)	N/A	N/A	N/A	X
	Core/Exit Router	N/A	N/A	N/A	N/A
	Gateway Router	N/A	X	N/A	N/A
Circuit Simulcast Prime Site Router		X	X	X	N/A
IP Simulcast Prime Site Routers:	Prime Site Router	X	X	N/A	N/A
	Remote Site Access Router (Ethernet-only subsite links)	N/A	N/A	N/A	N/A
	Dispatch Console Site Router	X	N/A	N/A	N/A
GGSN Router		N/A	N/A	N/A	N/A
Conventional Master Site (K core) GGSN Router		N/A	N/A	N/A	N/A

1.8.6
Replacing an Optional I/O Module – S6000

Replacing an optional I/O module in the S6000 chassis consists of removing the cover of the chassis, exchanging the modules, and replacing the cover on the S6000 chassis. Before performing this task, familiarize yourself with the Electrostatic Discharge (ESD) precautions.

Prerequisites: Consider:

⚠ **CAUTION:** ESD PRECAUTIONS
When removing or installing modules, take the following precautions to prevent Electrostatic Discharge (ESD) from damaging the internal components of the router:

- Always wear a properly grounded Electrostatic Discharge (ESD) wrist strap.
- Transport static-sensitive components in anti-static packaging.
- Keep static-sensitive components in their anti-static packaging until you are ready to install them.
- Just before removing components from their anti-static packaging, discharge static electricity from your body by touching an unpainted metal surface.
- When you handle modules, place them with the printed circuit side down on a nonconducting, static-free, and flat surface.

When and where to use: Replace the I/O module when it fails to operate properly or you are replacing an S6000 router as a unit.

IMPORTANT: Do not store unused or unconfigured I/O modules in unused router slots.
If you remove an I/O module, replace it with a module of the same type. For example, if you remove a FlexWAN module, replace it with another FlexWAN module, not an UltraWAN module. Similarly, if you replace an S6000 router as a unit, the replacement router must have the same hardware configuration (that is the same I/O modules installed in the same I/O module slots).

For the list of optional modules, see Field Replaceable Units – S6000 on page 62.

NOTICE: If the MNR S6000 is configured for use in a secure (Common Criteria) environment, the device is equipped with tamper evidence labels, which will be broken if you perform the following procedure. Contact Motorola Solutions to order replacement labels (part number TYN4008A), and follow the instructions provided with the labels to reapply them.

Procedure:

1. Power down the existing router by disconnecting the power cable from the router.

   DANGER: Shock hazard: Routers contain dangerous voltages, which can cause electrical shock or damage to equipment. Turn off the router and remove the power cabling when servicing this equipment.

   IMPORTANT: If the S6000 is configured with redundant power supplies (model numbers lower than CLN1780A), unplug both power cords to completely remove power from the S6000.

2. Remove the cover from the S6000 chassis.

   a. If mounting brackets are present, remove them from the chassis.

   b. Remove the two screws that secure the cover to the chassis.

      NOTICE: S6000 routers with model numbers lower than CLN1780A ship with redundant power supplies. The rear panel of these routers features two power connectors.

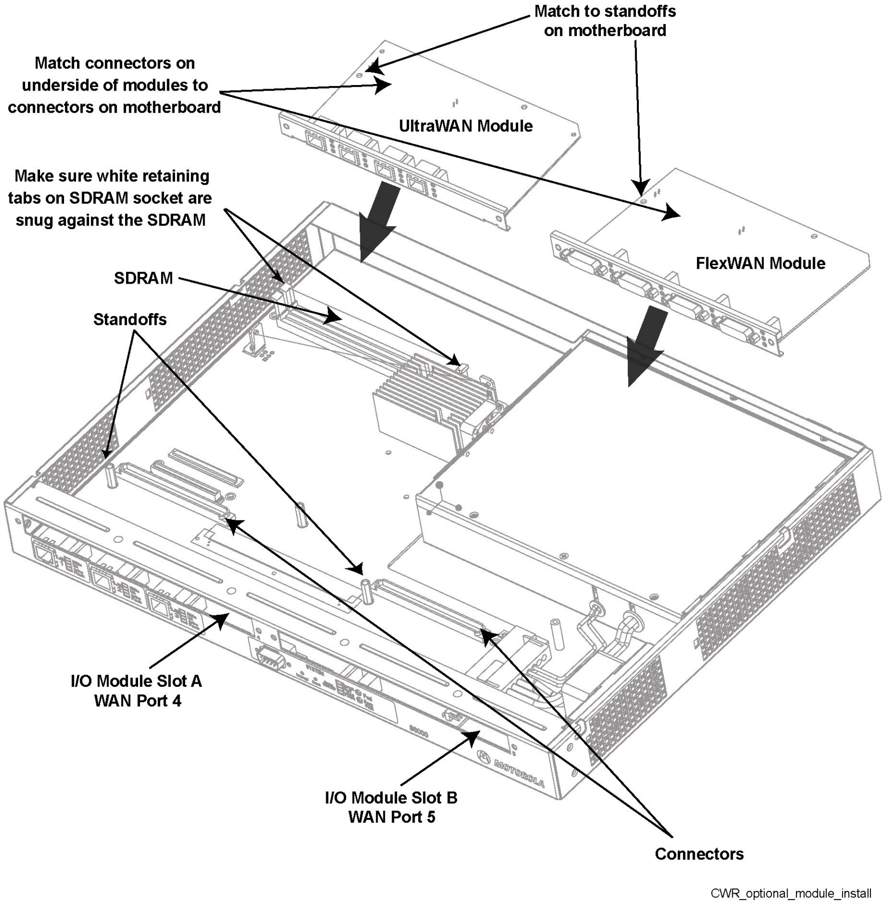
   c. Remove the cover from the chassis.

3. Remove the existing module:

   a. Locate the module you want to replace and remove the screws from the standoff. Set the screws aside, as they are needed later in this task

   b. Gently remove the module from the connector pins by pulling the connector up and off.

Figure 11: I/O Module Slot, Connector, and Standoff Locations on the S6000 Motherboard


Match to standoffs on motherboard
Match connectors on underside of modules to connectors on motherboard
UltraWAN Module
Make sure white retaining tabs on SDRAM socket are snug against the SDRAM
FlexWAN Module
SDRAM
Standoffs
I/O Module Slot A WAN Port 4
I/O Module Slot B WAN Port 5
Connectors
CWR_optional_module_install

4 Insert the new modules.

NOTICE: If you install a module in the I/O module slot B, make sure that the power supply wires for the fan are under the card when you insert it.

For each module that you install, perform the following actions:

a Insert the front of the module through the front panel of the chassis.

b Line up the connector pins carefully.

c Press down gently on the module.

5 Using a torque screwdriver, secure the module to the standoffs with the two screws and washers provided with the module.

IMPORTANT: To ensure that the module is seated properly, tighten the screws to a torque of 6.5 to 8.5 inch-pounds.

6 Using a Phillips screwdriver, secure the module to the front of the chassis with the two screws you removed in step 3.

7 Check the seating of the SDRAM to make sure that it was not nudged or unseated during the module installation. The white retaining tabs on the SDRAM socket should be snug against the SDRAM. The location of the SDRAM on the S6000 motherboard is illustrated in step 3.

8 Replace the cover and secure it to the chassis with the two screws you removed in step 2.

Postrequisites: Power up the router and verify that the replaced module is working properly.

Chapter 2

S2500 Introduction, Installation, and Configuration

This chapter provides a high-level description of the S2500 router and describes its features.

NOTICE: The S2500 platform does not support IPv6 and should not be used for encrypted site links requiring 128 bit encryption key strength.
The GGM 8000 platform is recommended for use after ASTRO® 25 7.9 System Release.

2.1 S2500 Physical Description

This section describes the physical hardware for the router.

2.1.1 Front Panel Description – S2500

The front panel of the S2500 remote site router features the following components:

Service Interfaces

Supports one Ethernet interface and up to three additional interfaces, depending on the hardware configuration. Slot A supports optional FlexWAN or T1/E1 modules. Slot B supports optional FlexWAN or T1/E1 modules. The analog slot supports an optional 4-port E&M module.

Console port

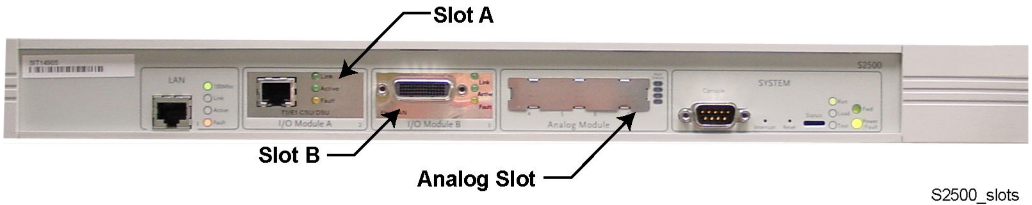
Connects the remote site router to a PC, terminal, or modem.

LED Indicators

Indicate the router interface and system status information.

The following figure shows the S2500 router with two I/O modules: the T1/E1 (Slot A) and FlexWAN (Slot B) respectively. The analog slot is empty.

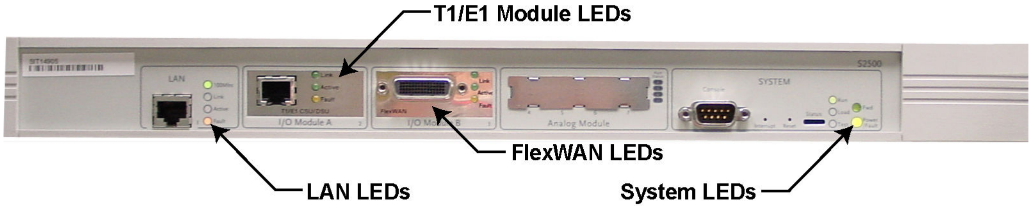
Figure 12: S2500 Router I/O Module Slot Locations



S2500_slots

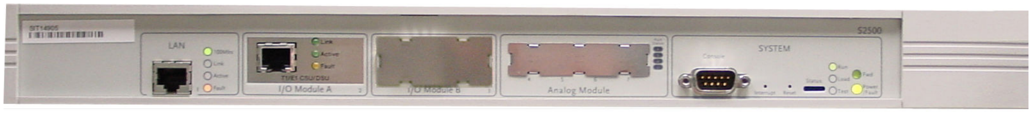
The following figure shows an example of the LEDs on the S2500 router.

Figure 13: S2500 Router LEDs



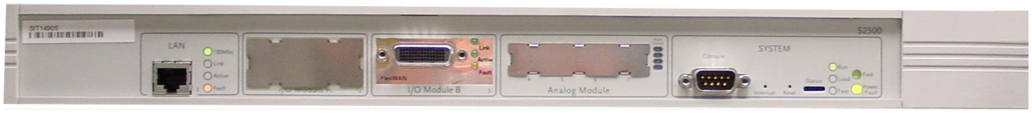
S2500_LEDs

Figure 14: S2500 Router with T1/E1 Port



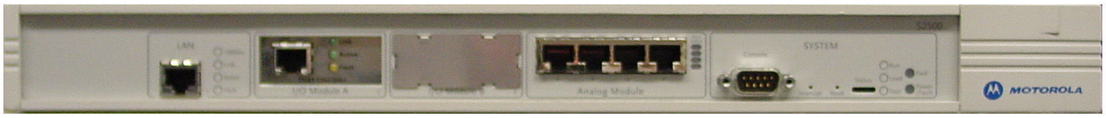
HPD_S2500_router_T1E1

Figure 15: S2500 Router with FlexWAN Port



HPD_S2500_router_flexwan

Figure 16: S2500 Router with E&M Module



S2500_router_front

NOTICE: See S2500 Troubleshooting on page 87 for details about the LEDs for different router configurations.

2.1.2 Rear Panel Description – S2500

The rear panel of the S2500 site router includes the following:

- Power receptacle
- Configuration label
- Grounding (earthing) screw

2.1.3 S2500 Router – Physical Specifications

Table 16: S2500 Router – Physical Specifications

S2500 Router	Specifications
Physical dimensions	Height: 4.3 cm (1.7 in.)
	Width: 30.5 cm (12.0 in.)
	Depth: 43.0 cm (16.9 in.)
Weight	4.54 Kg (10 lb)

2.1.4 S2500 Router – Environmental Specifications

You must adhere environmental requirements when installing the router.

IMPORTANT: The S2500 router requires proper ventilation and space to accommodate cabling requirements.

Table 17: S2500 Router – Environmental Specifications

Environmental Characteristic	Minimum Requirement	Maximum Requirement
Operating Temperature	0° C (32° F)	50° C (122° F)
Non-operating Temperature	-30° C (-22° F)	60° C (140° F)
Operating Altitude	N/A	3,048 m (10,000 ft)
Non-operating Altitude	N/A	12,192 m (40,000 ft)
Relative Humidity – Operating	5% non-condensing	95% non-condensing
Relative Humidity – Non-operating	5% non-condensing	95% non-condensing
Power Requirements	100 VAC	240 VAC
Thermal	N/A	136 BTU/hr
Heat Dissipation	N/A	40 Watts
Vibration	N/A	0.25G, Sine wave, 5-500-5 Hertz

2.2

S2500 Router Types

Routers used at remote sites handle various types of network traffic.

Table 18: Routers by System Location and Function

Location	Function	Comments
Circuit Simulcast Remote Site	Circuit Simulcast Remote Site router:	
	Prime site interface only	Handles network traffic between the prime site and remote site without the need to support circuit-based Conventional channels or remote console sites.
	Circuit-based Conventional channel support	Handles network traffic between the prime site and remote site with support for sites with a circuit-based Conventional channel.
	Analog CCGW	Supports up to 4 Analog conventional channels at the site.
	Digital CCGW	Supports up to 2 Digital Conventional channels at the site.

Location	Function	Comments
IP Simulcast Remote Site	IP Simulcast Remote Site Router:	
	Prime site interface only	Handles network traffic between the prime site and remote site without the need to support a circuit-based Conventional channel or remote console sites.
	Circuit-based Conventional channel support	Handles network traffic between the prime site and remote site with support for sites with a circuit-based Conventional channel.
	Analog CCGW	Supports Analog conventional channels at the site.
	Digital CCGW	Supports ASTRO® 25 system Conventional Digital channels at the site.
ASTRO 25 Repeater Site	Repeater Site router:	
	Master site interface only	Handles network traffic between the master site and remote site without the need to support a circuit-based Conventional channel or remote console sites.
	Circuit-based Conventional channel support	Handles network traffic between the master site and remote site with support for sites with a circuit-based Conventional channel.
	Analog CCGW	Supports Analog conventional channels at the site.
	Digital CCGW	Supports ASTRO® 25 system Conventional Digital channels at the site.
ISSI.1 Site	ISSI.1 Site Router:	
	Master site interface only	Handles network traffic between the master site and remote site without the need to support a circuit-based Conventional channel or remote console sites.
Dispatch Console Site	Dispatch Console Site router – Remote dispatch or Network Management (NM) Site support with Plant 911 support at master site	Handles network traffic between the prime site and remote site with support for remote dispatch or network management equipment.
	Master site interface only	Handles network traffic between the master site and remote site without the need to support a circuit-based Conventional channel or remote console sites.
	Analog CCGW	Supports Analog conventional channels at the site.
	Digital CCGW	Supports ASTRO® 25 system Conventional Digital channels at the site.
HPD Remote Site	HPD Site router:	

Location	Function	Comments
	Master site interface only	Handles network traffic between the master site and remote site without the need to support a circuit-based Conventional channel or remote console sites.
	Circuit-based Conventional channel support	Handles network traffic between the master site and remote site with support for sites with a circuit-based Conventional channel.
	Analog CCGW	Supports Analog conventional channels at the site.
	Digital CCGW	Supports ASTRO® 25 system Conventional Digital channels at the site.
Conventional Only Site	Conventional RF Site Router:	
	Master site interface only	Handles network traffic between the master site and remote site without the need to support a circuit-based Conventional channel or remote console sites.
	Circuit-based Conventional channel support	Handles network traffic between the master site and remote site with support for sites with circuit-based Conventional channels.
	Analog CCGW	Supports Analog conventional channels at the site.
	Digital CCGW	Supports ASTRO® 25 system Conventional Digital channels at the site.

2.2.1

Information Assurance Features Overview

The applicable Information Assurance (IA) features are included in different appropriate manuals.

NOTICE: Border Router and Peripheral Network Router do not have IA configurations, for example, they do not need SNMPv3 for fault management.

Table 19: Information Assurance Features

IA Feature	Related Manual
Router encryption and authentication (to filter traffic based on originating host), including Router Encryption Card Configuration	*Link Encryption and Authentication* manual
SSH (for secure data transfer)	*Securing Protocols with SSH* manual
Remote Authentication Dial-In User Service (RADIUS) client configuration	*Authentication Services* manual
SNMPv3 for fault management in the Unified Event Manager (UEM)	*SNMPv3* manual
Router Access Control Lists (ACLs) to encrypt links	*Information Assurance Features Overview* manual
Centralized Event Logging	*Centralized Event Logging* manual

2.3 S2500 Installation

Installation procedures for S2500 routers that are common to all S2500 router applications.

2.3.1 Installing an S2500 Router in a Rack

Routers are rack-mounted to provide easy access during installation and cabling. The S2500 router takes 1 rack unit to mount (1 rack unit = 1.75 inches).

Prerequisites: Prepare:

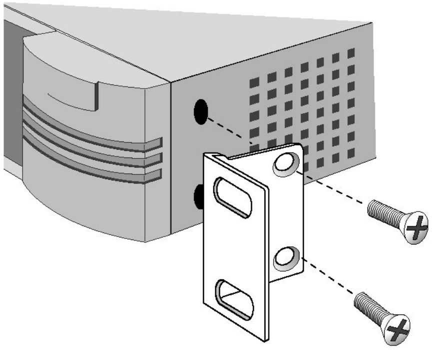
- Two rack-mount brackets
- Four 8/32 flathead Phillips screws
- Four panhead screws on each side (customer-provided)

CAUTION: Do not restrict air flow around the sides and back of S2500.

Procedure:

1. Secure the rack-mount brackets to each side of the chassis using two 8/32 flathead Phillips screws per bracket, as illustrated below.

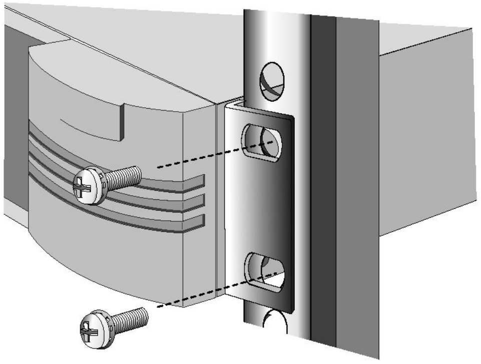
   Figure 17: Attaching the Rack-Mounting Screws

   S2500_rack_install_brackets

2. Hold the chassis between the poles of the rack and attach the brackets to the rack using panhead screws (you must provide these screws), as illustrated below.

Figure 18: Attaching the Router to the Rack



S2500_rack_install_screws

⚠ **CAUTION:** Using fewer than four screws (two on each side) to secure the brackets to the rack may cause the router to fall and sustain damage not covered by the warranty.

3 Tighten each screw securely.

Postrequisites: Before connecting the routers, ensure you have the required cabling and connectors.

⚠ **CAUTION:** Use only Category five unshielded twisted pair (or higher) cabling and connectors. Motorola Solutions has engineered this system to meet specific performance requirements. Using other cabling and connectors may result in unpredictable system performance or catastrophic failure!

2.3.2

S2500 Router – Power Connections

Table 20: S2500 Router – Power Specifications

Voltage	Consumption
100-240 VAC	40 W AC

2.3.2.1

Connecting the S2500 Router to the Power Source

The S2500 has a single, non-redundant power supply.

Prerequisites: Install the router on your system.

When and where to use: Power up the router and verify that it is working.

Procedure:

1 Connect the **female** end of a power cable to one of the power receptacles on the rear panel of the router.

2 Connect the **male** end of the power cable to the appropriate power source outlet (such as the AC outlet).

3 Verify that the power LED is on.

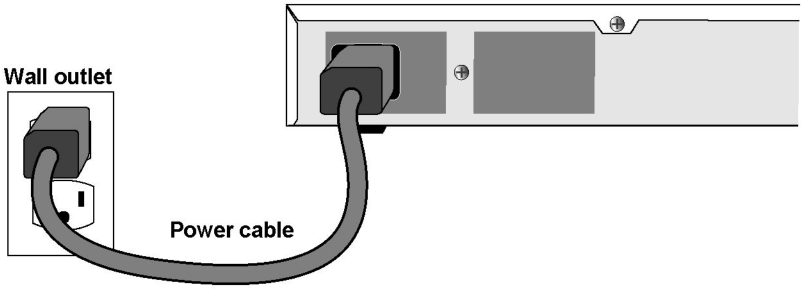
The power up process takes a few seconds. Successful completion of the process is indicated with the LEDs on the front panel of the router.

NOTICE: An appropriate device must be connected to the router, and powered on for the Local Area Network (LAN) LEDs to display properly.

See S2500 Troubleshooting on page 87 for further details about the LEDs.

NOTICE: Using a UPS backup power supply is recommended.

Figure 19: Cabling the Power Connector



S2500_power_connector_cabling

2.4 S2500 Configuration

This section provides configuration information for the S2500 router.

2.4.1 Router Software and Configuration Files Installation

The router's Enterprise Operating System (EOS) software and configuration files are installed at the factory. No additional installation is required.

If you replace a router, EOS software and configuration files have to be loaded on the new router after it is installed in the rack. If a firmware downgrade is necessary due to an MNR replacement, check the version of the firmware. Additional steps may be required depending on the firmware version. See Performing a Firmware Downgrade on page 250.

- If the router has no connectivity to the Unified Network Configurator (UNC) through the network, reload the files locally at the router using a service laptop and the configuration files provided by Motorola Solutions.
- If the router has connectivity to the UNC through the network, reload the files from the UNC, provided they were "pulled" to this application from the router before the failure.

For routers that are managed by UNC, see the *Unified Network Configurator* manual to learn about updating EOS images and software.

2.4.2 Router Configuration

This process explains how to load a router configuration file on a new router.

2.4.2.1 Configuration Prerequisites

You need to obtain certain items before you load a configuration file on a new router.

Table 21: Configuration Prerequisites

Prerequisite	Details
PC with a terminal emulation program and a 3com TFTP server application	Service technician's laptop
Ethernet crossover cable	To establish a LAN connection between the PC and the router
DB9 null modem cable	To establish console access between the PC and the router
Appropriate router configuration file for the router you are installing or replacing: `boot.cfg` (required), `StaticRP.cfg` and `acl.cfg` (if used)	Use the customized configuration files on the media device provided for your system by Motorola Solutions or backed up on your PC. For help in locating these files, contact your system administrator.
IP address for the router	Contact your system administrator for this information.
Account logins and passwords	Contact your system administrator for this information.

Configuration Prerequisites – Cautions and Notes

CAUTION: Do not tamper with the factory configuration settings for these devices. This includes software configuration, firmware release, and physical connections. Motorola Solutions has configured and connected these devices to meet very specific performance requirements. Tampering with these devices may result in unpredictable system performance or catastrophic failure.

NOTICE: Routers are configured at the factory. No additional configuration is required other than restoring the routers in the event of a break-fix situation. Field configuration of site routers is allowed, but you must contact the Motorola Solutions Support Center (SSC) for the configuration of routers at the master site or for the configuration of transport network devices at the remote site.

2.4.2.2 Configuring the S2500 Router

This process explains how to load a router configuration file on a new router.

Prerequisites: If necessary, contact your system administrator for prerequisite information.

When and where to use: Motorola Solutions routers are shipped from the factory with the appropriate Enterprise OS (EOS) installed. If you replace a router in the field and it is not possible to configure the replacement router at the factory, or if you need to load a router configuration file onto a new router during installation, follow this process.

Process:

1. Review the configuration prerequisites. See Configuration Prerequisites on page 35.
2. Determine the set of configuration files that is needed. See Configuration Files – S2500 on page 75.
3. Configure the IP address. See Configuring the IP Address and Workstation Connections on page 37.
4. Set up the 3Com TFTP application. See Configuring TFTP on page 38.
5. Transfer the configuration file. See Transferring the Router Configuration File on page 39.
6. Verify that the router rebooted and is running the new configuration. See Verifying the New Configuration on page 40.
7. Complete the router configuration. See Completing the Configuration on page 40.

2.4.2.3

Configuration Files – S2500

Different sets of configuration files applies for different S2500 router types.

S2500 Router	Configuration Files Set
Circuit Simulcast Remote Site router	boot.cfg acl.cfg
IP Simulcast Remote Site Router	boot.cfg acl.cfg
Repeater Site router	boot.cfg acl.cfg StaticRP.cfg
ISSI.1 Site Router	boot.cfg acl.cfg StaticRP.cfg
Dispatch Console Site router	boot.cfg acl.cfg StaticRP.cfg
HPD Site router	boot.cfg acl.cfg StaticRP.cfg
Analog CCGW	boot.cfg acl.cfg StaticRP.cfg
Digital CCGW	boot.cfg

S2500 Router	Configuration Files Set
	acl.cfg StaticRP.cfg
Conventional RF Site Router	boot.cfg acl.cfg StaticRP.cfg

2.4.2.4

Configuring the IP Address and Workstation Connections

You have to perform certain steps to configure the IP address for the router and connect it to a service workstation or laptop. Configure the IP address also when you replace a router in the field and load the router configuration file on a new router during installation.

Prerequisites: Install the router in the rack and ground it.
Connect the router to a power source and power it up.

Obtain:

- Ethernet crossover cable
- Null modem cable
- PC with a terminal emulation program

When and where to use: If you load a configuration file that changes the system IP address on an MNR router, the SNMPv3 credentials must be re-established with that router. Therefore, if SNMPv3 users were configured on the router before the system IP address change, you must issue the **ResetV3** command to reset the SNMPv3 data, then reconfigure the SNMPv3 users with the appropriate privilege levels. For details, see “Configuring MNR Routers and GGM 8000 Gateways for SNMPv3” in the *SNMPv3* manual.
After performing the **ResetV3** command to reset SNMPv3 data on an MNR router or GGM 8000 gateway, make sure to clear the USM cache. For details, see the “Accessing and Executing Existing Saved Commands” section in the *Unified Network Configurator* manual.

Clearing the cache does not apply to routers that do not use SNMP, which includes Border Routers or Peripheral Network Routers.

Procedure:

1 Assign the Ethernet port on the PC being used to perform the configuration:

- **IP Address**: 20.0.0.1
- **Subnet Mask**: 255.255.255.0

2 Connect the following cables between the PC and the router:

- Ethernet crossover cable between the Ethernet port on the PC and the LAN 1 port on the front of the router.

  NOTICE: The crossover cable crosses over pins 1 and 2 to pins 3 and 6.

- Null modem cable between the serial port on the PC and the console port on the router.

3 Power up the router and establish communication using a terminal emulation program, such as ProComm+ or HyperTerminal.

4 In the terminal emulation program, perform the following actions:

a Enter: `9600 baud rate`

b Enter: `8 bit`

c Enter: `No parity`

d Enter: `1 stop bit`

Press ENTER several times until the `NetLogin:` prompt appears.

5. At the `NetLogin:` prompt, type the default account name, **`root`**. Press ENTER.
6. At the `Password:` prompt, press ENTER. No password is necessary on an unconfigured router.

   The `EnterpriseOS#` prompt appears.

   NOTICE: The password for unconfigured routers is not defined.

7. Verify that the router is unconfigured (no IP addresses are assigned to any of the ports) by typing `sh -ip net`. Press ENTER.

   NOTICE: If there are any IP addresses defined, you must use the:
   `del !`***`<portlist>`***` -ip net `***`<ip address>`***

   command to delete them before continuing with this procedure.

8. To configure the IP address for the router, type the following command and press ENTER:

   ```
   setd !1 -ip net = 20.0.0.2 255.255.255.0
   ```

   NOTICE: The character after `setd !` is a number 1 (one).

   NOTICE: The IP addresses assigned in this procedure to the PC's Ethernet port and to the router have been chosen so that the router's IP address is on the same subnet as the PC used to configure this router.

2.4.2.5
Configuring TFTP

Configure the 3Com® TFTP server application when you replace a router in the field and load the router configuration file on a new router during installation.

Prerequisites: Use a dedicated site PC or laptop with 3Com TFTP server application.

Procedure:

1. Select and run the 3Com TFTP application from the Windows Program menu.

   The **3Com 3CServer** window appears.

2. From the TFTP toolbar, click **Setup**.

   The **3CServer Configuration** dialog box appears.

3. Select the **TFTP Configuration** tab.

   The **TFTP Configuration** tab appears.

4. Verify that the router configuration is present on the laptop computer, and that you know its location.
5. Select the router configuration file directory. In the **TFTP Configuration** tab, click **Browse Directories**, select the directory containing the router configuration files. Click **OK**.

2.4.2.6 Transferring the Router Configuration File

Transfer the router configuration file to the replacement router when you replace a router in the field and load the router configuration file on a new router during installation.

Prerequisites: Obtain:

- Appropriate router configuration files
- PC with a terminal emulation program

Procedure:

1 Return to the terminal emulator program. At the `EnterpriseOS#` prompt, type the following commands, and press ENTER after each command:

```
copy 20.0.0.1:<.cfg filename> a:/primary/boot.cfg
```

```
copy 20.0.0.1:<.cfg filename> a:/primary/<conf_file.cfg>
```

NOTICE:

- ***<.cfg filename>*** is the name of the router configuration file specific to the router you are replacing. For example, the configuration file for core router 1 in zone 1 is **z001core01.cfg**.
- ***<conf_file.cfg>*** is any additional configuration file you are using on the router. For example: acl.cfg or StaticRP.cfg. See Configuration Files – S6000 on page 36 or Configuration Files – S2500 on page 75 for a list of the configuration files required for each router, by network position. You must enter one copy command for each configuration file on the router. For example, if the router requires acl.cfg and StaticRP.cfg files in addition to the boot.cfg file, you would enter:

```
copy 20.0.0.1:<.cfg filename> a:/primary/boot.cfg
```

```
copy 20.0.0.1:<.cfg filename> a:/primary/acl.cfg
```

```
copy 20.0.0.1:<.cfg filename> a:/primary/StaticRP.cfg
```

The configuration files are transferred to the router, renamed as boot.cfg, acl.cfg and StaticRP.cfg (if used) respectively, and the `EnterpriseOS#` prompt reappears. The router now has the correct identity for the configuration.

2 Verify that the account password is set to the same value as the router.

3 Reboot the router to verify that the correct configuration files were loaded:

a Return to the terminal program.

b At the `EnterpriseOS#` prompt, type **`rb`** (ReBoot). Press ENTER.

The router reboots and processes the configuration files. Once complete, `System Initialized and Running` is displayed.

2.4.2.7 Verifying the New Configuration

When you replace a router in the field and load a router configuration file on a new router, reboot the router is rebooted and run the new configuration.

Prerequisites: Use a PC with a terminal emulation program.

Procedure:

1 After `System Initialized and Running` is displayed, log on to the router.

2 At the prompt, type `cd`. Press Enter.

3 At the `EnterpriseOS#` prompt, type `cat boot.cfg`. Press Enter.

4 Compare the Timestamp and Config Summary sections with the original file on the PC.

5 Type **`q`** to quit the display of the boot.cfg file. Press Enter.

6 Follow step 3 to step 5 for the rest of the configuration files for your router.

The router prompt now displays the system name of the router, rather than `EnterpriseOS#` and the information in the configuration files matches the original files.

7 Power down the router, disconnect the TFTP computer, and connect all system communication cables to the router. Power on the router.

2.4.2.8 Completing the Configuration

Perform certain steps to complete the process of configuring the routers.

Prerequisites: If appropriate, for the systems with link encryption or protocol authentication obtain:

- Pre-Shared Keys (PSKs)
- OSPF/PIM keys or OSPF-BGP keys
- SSH key

When and where to use: Follow this procedure if you replace a router in the field and wish to load a router configuration file on a new router during installation.

Procedure:

1 Power up the router.

The router reboots using the configuration files you loaded (such as, boot.cfg, acl.cfg, and StaticRP.cfg). The IP address you assigned to the router is replaced with the IP address specific to that router in your system.

2 On systems with MAC port locking, disable the locking on the LAN switch, and then re-enable the locking on the switch with the MAC address of the new router. For instructions on how to disable and enable MAC port locking, refer to the *MAC Port Lockdown* manual.

3 On systems with link encryption, enter the correct pre-shared keys (PSKs) for the new router so that it can be authenticated by its encryption peer. For instructions, refer to the *Link Encryption and Authentication* manual.

4 On systems that require SSH, generate a key for the new router to enable the SSH. For instructions, refer to the *Securing Protocols with SSH* manual.

5 For the centralized authentication feature, the RADIUS authentication sources are already set up in router configuration files by Motorola Solutions. The only RADIUS configuration you need to perform on Motorola Solutions routers is to enter the secret key that matches the “shared secret” for this RADIUS client on the RADIUS server. For instructions, see the *Authentication Services* manual.

6 On systems with SNMP Version 3 enabled, enable SNMPv3 passphrases. For instructions, refer to the *SNMPv3* manual.

7 On systems with protocol authentication, enter the correct OSPF/ PIM or OSPF/BGP keys for the new router so that it can authenticate with its authentication neighbor/peer. For instructions, refer to the *Link Encryption and Authentication* manual.

8 Discover the router in the UNC (if the UNC application is present in the system), refer to the *Unified Network Configurator* manual.

9. Upload the device configuration and hardware information from the router to the UNC. Refer to the “Scheduling the Pull of Device Configurations” section in the *Unified Network Configurator* manual.

Postrequisites: Verify that the router is operating properly.

NOTICE:
Routers are optimized at the factory. No additional optimization procedures are required for the routers.

For routers that are not managed by UNC, store configuration and hardware information from the router locally. Files must be backed up locally as the border router and peripheral network routers exist outside the Motorola Solutions RNI and are not configured or managed by the UNC application.

For routers that are managed by UNC, print out all the router configurations in your system from the UNC and store them in a secure location. If any router upgrades are made, print out the new configurations and replace those routers' records in your records. This provides specific address information for the individual routers. See the *Unified Network Configurator* manual or online help for more information.

For security purposes, all default passwords have to be changed prior to operational use. Those include both 'root' and 'admin' user passwords.

2.4.3
Updating Access Control List Files to Support System Expansions

System expansions require that you update the router access control list (ACL) files (`acl.cfg`) in different scenarios.
These scenarios are:

- Console site expansion – When you add a console site to a trusted group, you must update the `acl.cfg` file for all routers in the trusted group.
- Zone core expansion – When you add a zone core, you must update the `acl.cfg` file for all routers.

Prior to the ASTRO® 25 7.13 system release, the ACL update procedure involved copying the new `acl.cfg` file to the routers and rebooting the routers. The ASTRO®25 7.13 system release introduces the `antiacl.cfg` file, a file that completely removes the current `acl.cfg` settings from a router. By copying the `antiacl.cfg` file and the new `acl.cfg` file to a router, you can update the current ACL/ firewall settings without a reboot. You can perform the update procedure manually and automatically.

When and where to use: Update the ACL files in one of the following ways:

- Automatically, in the UNC (M core, or L core systems). For more information, see Automatically Updating Access Control List Files on page 42.

  NOTICE: Downtime cannot be avoided for L1 and M1 systems.

- Manually, using the router command line (K core systems). For more information, see Manually Updating Access Control List Files on page 43.

The following basic process steps are common for manual and automatic ACL updates.

NOTICE: The ACL file distribution and file activation can be implemented as two separate processes and executed at different times.

Procedure:

1. Distribute the antiacl.cfg and new `acl.cfg` files to the routers.
2. Activate the antiacl.cfg and new `acl.cfg` files.

3 Delete the antiacl.cfg file.

4 For a console site expansion, reboot the core router or routers. For a zone core expansion, reboot the exit router or routers.

> **NOTICE:** For systems that are redundant in the core, you must reboot both routers in the core or exit router pair. The gateway router does not require a reboot.

Related Links

Automatically Updating Access Control List Files on page 81

Manually Updating Access Control List Files on page 81

2.4.3.1 Automatically Updating Access Control List Files

You can use Unified Network Configurator (UNC) to automatically update Access Control List (ACL) files. You update the files without rebooting the router.

Prerequisites:
Familiarize yourself with the overview information. See Updating Access Control List Files to Support System Expansions on page 41.

Obtain the `antiacl.cfg` and new `acl.cfg` files, from your Motorola Solutions field representative.

When and where to use: Perform this process to support console site expansion or zone core expansions for ASTRO® 25 systems that employ the M core or L core zone cores.

Process:

1 Load the antiacl.cfg and new `acl.cfg` files to the UNC workspace. See the *Unified Network Configurator* manual for information about uploading the configurations for transport devices in the UNC Wizard.

2 Distribute the antiacl.cfg and new `acl.cfg` files to the impacted routers using UNC. Refer to the *Unified Network Configurator* manual for information about distributing configurations for transport devices by using the UNC Wizard.

> **NOTICE:** You can schedule many distributions of the configuration files. However, when you schedule a very large number of distributions, you may delay other UNC operations.

3 Clear old ACL and activate new ACL files using the UNC Save Command. Refer to the *Unified Network Configurator* manual for information about activating new ACL files.

4 Check the Activation Status of the ACL file. See the *Unified Network Configurator* manual for information about accessing and executing existing saved commands.

Return to Process

Updating Access Control List Files to Support System Expansions on page 80

Related Links

Manually Updating Access Control List Files on page 81

2.4.3.2 Manually Updating Access Control List Files

You can use Unified Network Configurator (UNC) to manually update Access Control List (ACL) files. You update the files without rebooting the router.

Prerequisites:

Familiarize yourself with the overview information. See Updating Access Control List Files to Support System Expansions on page 41.

Obtain the `antiacl.cfg` and new `acl.cfg` files from your Motorola Solutions field representative.

When and where to use: Perform this process on each of the impacted routers to support Console Site Expansion or Zone Core Expansions for ASTRO®25 systems that employ the K core.

Procedure:

1. Use TFTP (non-secure) or PuTTY secure copy protocol (SCP) (secure) to transfer `antiacl.cfg` and `acl.cfg` files to the impacted routers.

   See Transferring the Router Configuration File on page 39.
2. Establish a Telnet (non-secure) or SSH (secure) connection to the router.
3. Activate the antiacl.cfg file. From the router command line, enter:

   ```
   cd
   ```

   ```
   lc antiacl.cfg ie
   ```
4. Check the status of the antiacl.cfg file activation. From the router command line, enter:

   ```
   cat config.log | grep –i error
   ```
5. Activate the new `acl.cfg` file. From the router command line, enter:

   ```
   cd
   ```

   ```
   lc acl.cfg ie
   ```
6. Check the status of the `acl.cfg` file activation by repeating step 4.
7. Delete the `antiacl.cfg` file. From the router command line, enter:

   ```
   rf antiacl.cfg
   ```
8. Perform one of the following actions:
   - For a console site expansion, reboot the core router or routers.
   - For a zone core expansion, reboot the exit router or routers.

Return to Process

Updating Access Control List Files to Support System Expansions on page 80

Related Links

Automatically Updating Access Control List Files on page 81

2.4.4 Router Configuration in the Unified Network Configurator

The Unified Network Configurator (UNC) resides on the User Configuration Server (UCS). You use UNC to perform various actions.

Use UNC to:

- Group the routers to perform the following tasks on more than one router at a time, including:
  - Backing up and restoring routers.
  - Rebooting one or more routers.
- Maintain router configuration and software files, view router information, and launch telnet sessions.
- Prepare the router for management and to configure managed routers. Refer to the *Unified Network Configurator* manual for the following procedures:

- Preparing the router for management, see the “Configuration Management” section.
- Restoring a previous router configuration, see the “Rolling Back to a Previous Version” section.
- Changing a current router configuration and send it to the router, see the “Device Update with a Download of Configuration Changes” section.

NOTICE: This topic does not apply to the Border Router or Peripheral Network Routers.

2.4.5

Backing up the Router Configuration

You can create a backup of the router’s running configuration files and execution image by copying the contents of the router’s primary directory either to the router’s secondary directory or to a TFTP server. This backup includes the Motorola Solutions-provided configuration files as well as other manually-entered configuration, such as pre-shared keys. In the event that the contents of the router’s primary directory are corrupted, you can restore the configuration files and execution image from the backup.

Use these procedures to create backups which you can use to recover the router configuration in the event of a failure.

NOTICE: The backups created by these procedures are specific to the physical motherboard from which the primary directory contents are copied. In other words, these backups work only if the motherboard from which you copied the configuration files and execution image is installed in the device you are restoring. You cannot use the backups created by these procedures if you are swapping one device for another or if you are replacing a motherboard.

2.4.5.1

Creating a Local Backup

To create a local backup, use the following procedure to copy the contents of the router’s primary directory to the router’s secondary directory.

Prerequisites: PC with a terminal emulation program.

Procedure:

1. At the `EnterpriseOS#` prompt, enter the following command to clean up the previous backup:

   ```
   RF a:/secondar/*.*
   ```

2. Enter the following command to make a copy of the current running configuration and execution image:

   ```
   COPY a:/primary/*.* a:/secondar
   ```

3. Check if there are any subdirectories of the **a:/primary** directory. If so, repeat steps 1 and 2 above for each subdirectory, replacing **`a:/primary/`** with the path to the subdirectory in the **`COPY a:/primary/*.* a:/secondar`** command.

4. To subsequently restore the router configuration from the backup in the secondary directory in the event that the contents of the primary directory have become corrupted, follow these steps:

   a From the `EnterpriseOS#` prompt, enter `SF 7` to open the **SysconF** command Boot Sources menu.

   b Enter 3 to direct the router to boot from the secondary directory.

   c Reboot the router.

2.4.5.2 Backing Up to a TFTP Server

To back up the contents of the router's primary directory to a TFTP server, use the following procedure.

Prerequisites: Dedicated site PC or laptop with TFTP server application.

Procedure:

1. Connect a straight-through Ethernet cable between the router and a hub or switch port that is in the same subnet as the TFTP server.
2. At the `EnterpriseOS#` prompt, enter the following commands to configure the router to access the TFTP server:

   ```
   SETDefault !3 -IP NETaddr = <IP address> [<network mask>]
   ```

   Where ***<IP address>*** is the IP address you want to assign to the router's Ethernet port and ***<network mask>*** is the subnet mask.

   ```
   SETDefault !3 -PAth CONTrol = Enable
   ```

   ```
   SETDefault !3 -POrt CONTrol = Enable
   ```

   ```
   ADD -IP ROUte <IP address> <mask> <gateway> <metric>
   ```

   Where ***<IP address>*** is the subnet address for the TFTP server, ***<mask>*** is the subnet mask, ***<gateway>*** is the gateway IP address, and ***<metric>*** represents the number of hops required for a packet to reach its destination.

   Step example:

   ```
   SETDefault !3 -IP NETaddr = 10.79.130.128 255.255.255.0
   SETDefault !3 -PAth CONTrol = Enable
   SETDefault !3 -POrt CONTrol = Enable
   ADD -IP ROUte 10.79.0.0 255.255.0.0 10.79.130.1 0
   ```

3. Enter the following command to generate a list of files in the router's primary directory: **`DF a:/primary`**
4. Use the list of file names generated in step 3 to create a list of copy commands, one command for each file name, and enter them one at a time until all the files in the list have been copied.

   Step example:
   For example, if the list returned by the DF command consists of a boot.ppc file and a boot.cfg file, enter the following commands to copy the files to a directory named backup1 on the TFTP server with IP address 10.79.0.2:

   ```
   copy a:/primary/boot.ppc 10.79.0.2:/backup1
   copy a:/primary/boot.cfg 10.79.0.2:/backup1
   ```

   NOTICE: If the list returned by the DF command includes other files in addition to the boot.ppc and the boot.cfg files, then you must enter additional copy commands (one command for each file), substituting the filename(s) of the additional files for boot.ppc or boot.cfg in the examples above.

5. To subsequently restore the router configuration files and execution image from the backup on the TFTP server in the event that the contents of the router's primary directory have become corrupted, follow these steps:

   a. From the `EnterpriseOS#` prompt, enter a copy command for each file in the backup directory. For example, if backup directory backup1 on the TFTP server with IP address 10.79.0.2 includes a boot.ppc file and a boot.cfg file, enter the following commands:

```
copy 10.79.0.2:/backup1/boot.ppc a:/primary
```

```
copy 10.79.0.2:/backup1/boot.cfg a:/primary
```

NOTICE: If the backup directory includes other files in addition to the boot.ppc and the boot.cfg files, then you must enter additional copy commands (one command for each file), substituting the filename(s) of the additional files for boot.ppc or boot.cfg in the examples above.

b Reboot the router.

2.4.6 Router Discovery by the Use of UEM

Once the router is discovered and configured in the Unified Network Configurator (UNC), the router must be discovered in the Unified Event Manager (UEM) for fault management. The active router is discovered as part of the subnet discovery. Refer to the *Unified Event Manager* manual for more information on this procedure.

NOTICE: The router must be discovered in the UEM for traps and events to appear in the UEM.

2.5 S2500 – Operation

This section details tasks that you perform once the router is installed and operational on your system.

2.5.1 Router Administration

You can administer routers in different ways.

Nearly all the necessary router administration can be performed in the Unified Network Configurator (UNC). For the information to locally set up the basic router configuration, refer to the *Unified Network Configurator* manual.

However, when the router does not have an established connection with the master site LAN or is not managed by UNC, you can administer basic router information, such as its IP address, gateway address and other configuration parameters in two ways:

- Through the terminal server menus
- Directly through a connection to the console port on the router

CAUTION: Do not tamper with the factory configuration settings for these devices. This includes software configuration, firmware release, password, and physical connections. Motorola Solutions has configured and connected these devices to meet very specific performance requirements. Tampering with these devices may result in unpredictable system performance or catastrophic failure.

For information on how to connect to a router through a terminal server emulator and configure the router IP address, see Configuring the IP Address and Workstation Connections on page 37.

2.5.2

Power Up – S2500 LEDs Status

Powering up the router takes a few seconds and when the process is successfully completed, the LEDs on the front panel display differently.

NOTICE: An appropriate device must be connected to the router and powered on for the Local Area Network (LAN) LEDs to display properly.

Table 22: LED Status after Successful Power Up

LED	Status
LAN	
Link	ON
Active	OFF or blinking
Fault	OFF
T1/E1 CSU/DSU	
Link	ON
Active	ON
Fault	OFF
SYSTEM	
Status	All OFF
Fwd	OFF or blinking
Power/Fault	Green
Run	ON
Load	OFF
Test	OFF

NOTICE: Depending on the I/O modules installed in the S2500 router, some of the status information may not apply to specific configurations.

2.6

S2500 Maintenance

This section describes periodic maintenance procedures relating to the router.

2.6.1

Maintaining Routers

The router does not contain serviceable parts that require maintenance or calibration. Maintaining requires only basic procedures.

Follow the basic rules for the router maintenance:

- Use a clean, lint-free cloth or a soft brush for exterior cleaning.
- Ensure that the ventilation ports are kept clean at all times.
- Monitor the router LEDs periodically to ensure that the router is operating properly.

NOTICE: It is also advisable to do periodic interior cleaning by using a low-suction vacuum cleaner.

2.7 S2500 Troubleshooting

This section provides fault management and troubleshooting information relating to the routers.

2.7.1 Troubleshooting the Router

The following resources are available for troubleshooting problems with the managed routers:

- Unified Network Configurator (UNC)
- Unified Event Manager (UEM)
- Local router administration (performing the task on the router through a direct connection to the console port on the router)

NOTICE: The Border Router and Peripheral Network Routers are not configured or managed by UNC or UEM. Actions must be performed locally as these routers exist outside the Motorola Solutions Radio Network Infrastructure (RNI).

See the *Unified Event Manager Online Help* for details on the alarms for the routers.

2.7.1.1 Troubleshooting General Connectivity Problems

Troubleshoot general connectivity problems by checking the alarms and physical connections or reloading the configuration files.

Prerequisites: Install and configure the router.

When and where to use: Use the following steps to troubleshoot the router's connectivity problems related to the LAN connection.

NOTICE: The Border Router and Peripheral Network Router do not support the UNC/UEM procedures. You can perform the same tasks locally using the router administration menus.

Procedure:

1. Perform the following actions:
   - In the Unified Event Manager (UEM), check the conditions and alarms for the router.
   - In the Unified Network Configurator (UNC), check the router configuration and router log information.
   - Verify that the IP address, MAC address, and other configuration settings are correct.
2. Using UEM, check the alarms for other critical network devices on the LAN. Also, verify the configuration of the LAN switch.
3. Check the physical connection to the LAN port on the router. Verify that the cabling is properly connected and in good condition.
4. Try to reboot the router through the UNC or cycle power to the router. See the *Unified Network Configurator* manual for more information.
5. If the router fails to establish a connection, power down the router, and test the Ethernet cable for continuity, attenuation, and excessive crosstalk. Replace the cable if necessary.

6. If the connection still fails, try to reload the EOS software and configuration files to the router locally or through the Unified Network Configurator (UNC). See the *Unified Network Configurator* manual for instructions.
7. If the router still fails to operate properly, replace the router.

2.7.1.2 Troubleshooting General Performance Problems on the LAN

Troubleshoot LAN performance problems of the routers by using the Unified Event Manager (UEM), Historical Reports, Performance Reports, InfoVista, or checking the physical connections.

Prerequisites: Install and configure the router.

When and where to use: Use the following steps to troubleshoot the router's performance problems on the LAN.

NOTICE: The Border Router and Peripheral Network Router do not support the UNC/UEM procedures. You can perform the same tasks locally using the router administration menus.

Procedure:

1. In the UEM, check the condition of the LAN switch and all affected devices and links. Verify that all the routers are operational.
2. Using Historical Reports and Performance Reports, check the overall loading of calls and activities on the LAN. Verify that the loading is within the maximum loading specifications for the system.
3. Using InfoVista, generate performance and traffic reports for the routers. Look for anomalies, heavy volumes of traffic, or high CPU utilization, or other device resources.

   NOTICE: InfoVista is an option for ASTRO® 25 systems. The Border Router and Peripheral Network Router do not support InfoVista.

4. Run ping, traceroute, pathping commands, and loopback testing across any troubled links or between any suspected devices.
5. Verify that the address tables, subnet masks, and default gateways are set correctly in the router and other networked devices.
6. Physically verify that the LAN switch is operating properly. Check the LEDs and physical connections, and verify that all cabling conforms to the standard. Check for sharp bends in cabling and cable length not adhering to the specification (such as 100 meters for 10Base-T).
7. Check the troubled cabling for noise, attenuation, continuity, and crosstalk. Verify that the communication cabling is routed apart from all power cabling and power sources. Verify that the cabling is also clear from any test equipment that may cause interference.
8. As applicable, verify that any service provider connections are providing the appropriate throughput for the system.
9. Identify the bottleneck points in the system. Check and reload device configurations as necessary, or replace any suspected switching or routing devices that may not be performing to specification.
10. Revise the configurations, services, and permissions for the subscribers as necessary.
11. Purchase additional equipment to handle the additional load of traffic (more routers or sites). Contact Motorola Solutions for assistance.

2.7.2 LED Indicators – S2500

The indication of each LED informs the user about the S2500 router status.

- **LAN LEDs** – Indicate the condition and activity for each of the Ethernet ports connected to the LAN.
- **T1/E1 Module LEDs** – Indicate the condition and activity for the T1/E1 module.
- **Ethernet 10Base-T Module LEDs** – Indicate the condition and activity for Ethernet 10Base-T module LEDs.
- **FlexWAN LEDs** – Indicate the conditions and activity for each FlexWAN port on the router.
- **System LEDs** – Indicate the overall condition of the router system, including its operating status, power conditions, and fault conditions.
- **E&M Module LEDs** – Indicate the condition and activity for the E&M module. E&M modules are only installed in the S2500 when the router is configured as an Analog CCGW
- **V.24 Module LEDs** – Indicate the condition and activity for the V.24 module. V.24 modules are only installed in the S2500 when the router is configured as a Digital CCGW.

NOTICE: For more information on the LEDs statuses, refer to the troubleshooting sections in this manual.

Table 23: S2500 Router LED Indications

LED Type	LED	LED Descriptions
LAN	100 Mbs	Illuminates **Green** when 100Base-TX Ethernet is in use.
	Link	Illuminates **Green** when the Ethernet link is established, that is, the path is up.
	Active	Flickers **Green** when a packet is detected, that is, the Ethernet port is receiving or transmitting packets.
	Fault	Illuminates **Amber** when an error is detected or the self-test has failed.
T1/E1 Module	Link	Illuminates **Green** when the path is up.
	Active	Illuminates **Green** when an end-to-end connection exists or is in progress.
	Fault	Illuminates **Amber** when an error in the frames is detected.
Ethernet 10Base-T Module	Link	Illuminates **Green** when the path is up.
	Transmit	Flickers **Green** when a packet is being transmitted on the LAN.
	Receive	Flickers **Green** when a packet is being received on the LAN.
	Collision	Illuminates **Amber** during system startup and initialization or when a collision occurs in half duplex mode.
FlexWAN	Link	Illuminates **Green** when the path is up.
	Active	Illuminates **Green** when there is a physical connection to a serial device.
	Fault	**OFF** in normal operation. Illuminates **Amber** when an error is detected in the frames or no cable is connected to the serial port.
System	Run	Illuminates **Green** when the software has successfully loaded and is running.

LED Type	LED	LED Descriptions
	Load	**OFF** in normal operation. Flickers **Green** during startup to indicate the system is loading software. Illuminates **Amber** when there is a load problem.
	Test	**OFF** in normal operation. Illuminates **Amber** during startup to indicate the system is running self-tests.
	Status	Provides additional status for the Run, Load, and Test LEDs. Four status LEDs show a code indicating specific types of loading failures. For the codes shown, zero (0) represents an extinguished LED and one (1) represents an illuminated LED.
	Forward (Fwd)	Flickers **Green** each time a packet is forwarded between ports.
	Power/Fault	Illuminates **Green** when the unit has power. Illuminates **Amber** if there is a problem with power. When unlit, power to the unit is **OFF**.
E&M Module	Port status	E&M modules are only installed in the S2500 when the router is configured as an Analog CCGW. The E&M module has four port status LEDs, each of which indicates the status of one of the four E&M ports, with the top LED indicating the status of the left-most port: • Illuminates **Green** – The analog channel corresponding to this port is enabled and idle. • Illuminates **Yellow** – The CCGW functionality is not enabled; the DSP is out of service; or a fault has been detected on the analog channel corresponding to this port. **NOTICE:** When the S2500 boots up, the E&M port LEDs are yellow until the first analog channel is configured. Once an analog channel is configured, the E&M port LEDs are off and turn yellow if an enabled/active channel fails. • **OFF** – CCGW functionality is enabled, but the channel corresponding to this port is disabled or is not configured to use an E&M port (for example, it is a V.24 digital channel). • Blinking **Green** – The analog channel corresponding to this port is enabled, and audio packets are flowing. **NOTICE:** For the E&M module port status LEDs to illuminate **Green**, the CCGW service must be enabled and the site type must be configured as **analog** from the LDAP server. Channel types are configured in the LDAP database through UCM.
V.24 Module	Port status	V.24 modules are only installed in the S2500 when the router is configured as a Digital CCGW. The V.24 module has two port status LEDs, each of which indicates the status of one of the V.24 ports: • Illuminates **Yellow** when the CCGW service is enabled and the corresponding channel is configured to use the V.24 port (it is a digital channel), but the V.24 port is not connected.

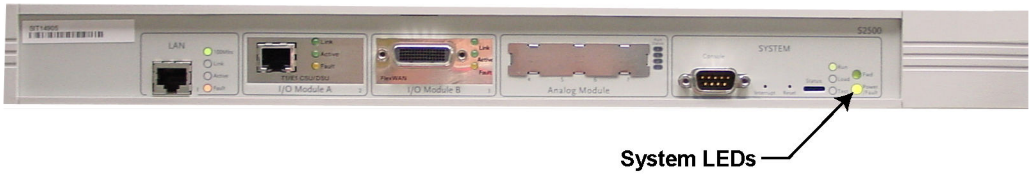
LED Type	LED	LED Descriptions
		• **Off** – The CCGW service is disabled or the corresponding channel is not configured to use the V.24 port (it is an analog channel). • Illuminates **Green** – The V.24 port is connected, the HDLC link is up, and the digital channel corresponding to this port is enabled and idle. • Flickering **Green** – The V.24 port is connected, the HDLC link is up, the digital channel corresponding to this port is enabled, and audio packets are flowing. **NOTICE:** For the V.24 module port status LEDs to illuminate **Green**, the CCGW service must be enabled and the site type must be configured as **digital** from the LDAP server. Channel types are configured in the LDAP database, through UCM.

2.7.3
System LEDs Troubleshooting – S2500

The indication of each LED informs the user about the S2500 router status. The System LEDs indicate the overall condition of the router system, including its operating status, power conditions, and fault conditions.

When a router failure occurs, the four Status LEDs can also indicate a failure code that defines the particular problem. The System LEDs are located near the console port on the front of the router. The four Status LEDs show a code indicating specific types of loading failures. For the codes shown, zero (0) represents an extinguished LED and one (1) represents an illuminated LED.

Figure 20: System LEDs



S2500_system_LEDs

Table 24: System LEDs

LED	Indication	Status and Troubleshooting Action
Run	Green	Indicates the router has successfully loaded, all startup diagnostics have passed, and the router is operating normally. No action is necessary.
	OFF	The router is not powered or is not running properly. **1** Use UEM to check the conditions and alarms for the router. **2** Verify that the Power/Fault LED is solid Green and the Load LED is OFF. • If the Power/Fault LED is extinguished, there can be a problem with the power input.

LED	Indication	Status and Troubleshooting Action
		• If the Load LED is illuminated, then there can be a loading problem. Follow the troubleshooting steps for these other LEDs for more information.
Load	OFF	Router is loaded and operating normally. No action is necessary.
	Flickering Green	Router is initializing. No action necessary.
	Amber	The router is experiencing a loading problem. This is typically accompanied by a solid Amber indication by the Power/Fault LED. The Status LEDs indicate the specific type of loading problem. See the Status LED troubleshooting steps for more information. **1** Using UEM or applicable fault management application, check the conditions and alarms for the router. **2** Cycle power to the router. **3** If the router continues to iterate through the boot process without finally moving into the run mode, contact the Motorola Solutions Support Center (SSC) for assistance.
Test	OFF	The router is operating normally. No action is necessary.
	Amber	The router is performing self tests. No action is necessary.
Status	0001	The router file system is empty. Try reloading the EOS software and configuration files through the UNC. See the *Unified Network Configurator* manual for instructions.
	0010	A read-only memory corruption is detected. Cycle power to the router and try reloading the EOS software and configuration files locally.
	0011	The software image file is deleted or the boot source and image names do not match. If the Test LED is also illuminated, the router is indicating an EEPROM checksum error. **1** Cycle power to the router and see if the condition is cleared. **2** If the condition does not clear, try reloading the EOS software and configuration locally. **3** If the problem is not resolved, replace the router or contact Motorola Solutions Support Center (SSC) for assistance.
	0101	The file size is larger than available memory. **1** Cycle power to the router and see if the condition is cleared **2** If the condition does not clear, try reloading the EOS software and configuration files locally. **3** If the problem is not resolved, replace the router or contact Motorola Solutions Support Center (SSC) for assistance.
	0100	A file read or decompression error has been detected. Cycle power to the router and try reloading the EOS software and configuration files locally.
	0110	A file checksum error has been detected. Cycle power to the router and try reloading the EOS software and configuration files locally.

LED	Indication	Status and Troubleshooting Action
	0111	An unspecified fatal error has occurred. **1** Cycle power to the router and try reloading the EOS software and configuration files locally. **2** If the router does not boot properly, use UEM or the applicable fault management application to check the alarms for the router. **3** If the router still fails to operate properly, replace the router.
Forward (Fwd)	Flickering Green	Packets are being forwarded between the two Ethernet ports. No action is necessary.
Power/ Fault	Green	The router is properly powered. No action is necessary.
	Amber	The router is reporting a fault condition. Troubleshoot the router according to the Load LED and Status LED troubleshooting instructions above. **1** Check the Load LED and Status LEDs for additional error indications. Use the troubleshooting steps for the Load LED or Status LEDs if they are illuminated. **2** Check the conditions and alarms for the router. Use UEM for managed routers. **3** Try rebooting the router through the UNC for managed routers or cycle power to the router. **4** If the router does not boot properly, try reloading the EOS software and configuration files locally. **5** If the router still does not run properly, replace the router.
	OFF	The router is not powered. **1** Check the conditions and alarms for the router. Use UEM for managed routers. **2** Connect the router to a different power source that is operational. Verify that the power cabling is firmly connected in the rear of the router. **NOTICE:** If possible, maintain redundant routers on separate circuits. **3** If the router still does not boot up, replace the router.

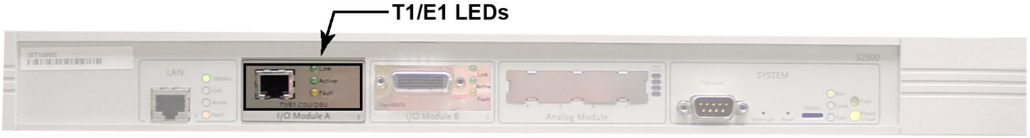
2.7.4

T1/E1 Module LEDs Troubleshooting – S2500

The fault conditions and activity of the T1/E1 port are related to the T1/E1 LED indication, which determines the relevant actions you need to take to troubleshoot the router. The T1/E1 Module is present, for example, when the router is used for master site interface only.

The LEDs indicate the carrier condition, loopback mode activity, and any alarms for the port. If no LEDs are illuminated, then the port is disabled.

Figure 21: T1/E1 LEDs



S2500_T1E1_LEDs

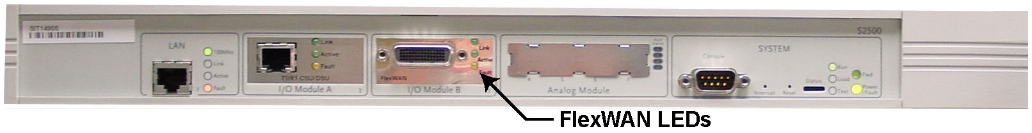
Table 25: T1/E1 LEDs

LED	Description	Indication	Status and Troubleshooting Action
Link	Indicates the condition of the T1/E1 link.	Green	The path is established. No action is necessary.
		OFF	A link failure has occurred (Active LED is illuminated), a loss of signal has occurred (Fault LED is illuminated), or the path/port has been disabled (no LEDs are illuminated). **1** If no LEDs are illuminated for the T1/E1 port, verify that the path/port is enabled. **2** Using UEM, check the conditions and alarms for the router. Also, check the router configuration and history of router configuration changes in UNC. Check the status of the equipment at the other end of the WAN link. **3** Check the physical connection to the T1/E1 port and verify that the cable is in good condition. **4** Contact the service provider to determine the WAN link status, or check the status of the transport equipment. **5** If necessary, try rebooting or cycling power to the router. **6** If the problem persists, contact Motorola Solutions for assistance.
Active	Indicates an active connection on the T1/E1 link.	Green	If the Link LED is illuminated, then the end-to-end connection exists and service is in progress. No action is necessary.
		Flickering Green	A loopback is initiated by a remote host over the link. No action is necessary.
Fault	Indicates when a loss of signal has occurred on the T1/E1 link.	Amber	Loss of signal has occurred. **1** Using UEM, check the conditions and alarms for the router. Also, check the status of the equipment at the other end of the WAN link. **2** Check the physical connection to the T1/E1 port and verify that the cable is in good condition. **3** Contact the service provider to determine the WAN link status, or check status of the transport equipment. **4** If necessary, try rebooting or cycling power to the router. **5** If the problem persists, contact Motorola Solutions for assistance.
		Off	No faults are detected. No action is necessary.

2.7.5 FlexWAN LEDs Troubleshooting – S2500

The FlexWAN LEDs indicate the conditions and activity for each FlexWAN port on the router. The FlexWAN port is used for the V.35 serial connection to the High-Speed Unit (HSU) card on the channel bank when a circuit-based Conventional channel is supported at the site.

Figure 22: FlexWAN LEDs



S2500_FlexWAN_LEDs

Table 26: Site Router – FlexWAN LEDs

LED	Description	Indication	Status and Troubleshooting Action
Link	Indicates whether the link is established.	Green	The link is established. No action necessary.
		Off	The link is not established for some reason. **1** Using UEM, check the conditions and alarms for the router. Also, check the router configuration and router log information in the UNC. Lastly, check the alarms and configuration for the device on the other end of the link. **2** Verify the configuration for the router in the UNC. If applicable, send an enable diagnostic command for the router through UEM. **3** Check the physical connection to the port. Verify that the cable is properly connected and in good condition. **4** Try to reboot the router through the UNC, or cycle power to the router. **5** If the port fails to establish a connection, power down the router and test the cable for problems, as possible. Replace the cable if necessary. **6** If the port still fails, try to reload the EOS and configuration files to the router through the UNC. **7** If the router still fails to operate properly, replace the router.
Active	Indicates that activity is detected on the port.	Green	Illuminates **Green** when there is a physical connection to a serial device. The port is sending and receiving traffic normally. No action is necessary.
		OFF	No activity is detected. If the port should be active, troubleshoot the router as explained for a Link LED failure above.
Fault	Indicates when a fault has been detected or the self-test for	OFF	The port is okay. No action is necessary.
		Amber	A fault has been detected or the self-test for the port has failed.

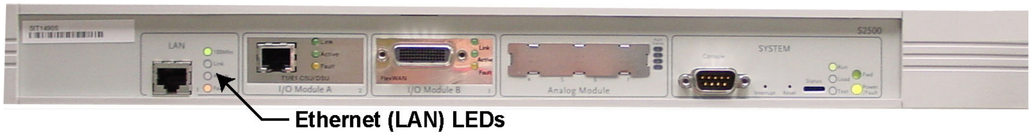
LED	Description	Indication	Status and Troubleshooting Action
	the port has failed.		**1** Using UEM, check the conditions and alarms for the router. Also, check router configuration and router log information in the UNC. **2** Check the physical connection to the port. Verify that the cable is properly connected and in good condition. Replace if necessary. **3** Try to reboot the router through the UNC, or cycle power to the router. **4** If the port still fails, try to reload the EOS and configuration files to the router through the UNC. **5** If the router still fails to operate properly, replace the router.

2.7.6

LAN LEDs Troubleshooting – S2500

The fault conditions and activity of the Ethernet (LAN) port are related with the Ethernet (LAN) LEDs indication, which determine the relevant actions you need to take to troubleshoot the router.

Figure 23: Ethernet (LAN) LEDs



S2500_FlexWAN_LEDs2

Table 27: Ethernet (LAN) LEDs

LED	Description	Indication	Status and Troubleshooting Action
Link	Indicates whether the link is established.	Green	The link is established. No action is necessary.
		OFF	The link is not established for some reason. **1** Using UEM, check the conditions and alarms for the router. Also, check the router configuration and router log information in the UNC. Also, check the alarms and configuration for the device on the other end of the link. **2** Verify the configuration for the router in the UNC. If applicable, send an enable diagnostic command for the router through the UEM. **3** Check the physical connection to the port. Verify that the cable is properly connected and in good condition. **4** Try to reboot the router through the UNC, or cycle power to the router. **5** If the port fails to establish a connection, power down the router and test the cable for problems, as possible. Replace the cable if necessary.

LED	Description	Indication	Status and Troubleshooting Action
			6 If the port still fails, try to reload the EOS and configuration files to the router through the UNC. **7** If the router still fails to operate properly, replace the router.
Active	Indicates that activity is detected on the port.	Flickering Green	The port is sending and receiving traffic normally. No action is necessary.
		OFF	No activity is detected. If the port should be active, troubleshoot the router as explained for a Link LED failure above.
Fault	Indicates when a fault has been detected or the self-test for the port has failed.	OFF	The port is okay. No action is necessary.
		Amber	A fault has been detected or the self-test for the port has failed. **1** Using the UEM, check the conditions and alarms for the router. Also, check router configuration and router log information in the UNC. **2** Check the physical connection to the port. Verify that the cable is properly connected and in good condition. Replace if necessary. **3** Try to reboot the router through the UNC, or cycle power to the router. **4** If the port still fails, try to reload the EOS and configuration files to the router through the UNC. **5** If the router still fails to operate properly, replace the router.
100 Mb	Indicates that 100BASE-TX Ethernet is in use.	Green	100BASE-TX is in use. No action is necessary.
		OFF	10BASE-T is in use. No action is necessary.

2.7.7

Ethernet 10Base-T Module LEDs Troubleshooting

The fault conditions of the Ethernet 10Base-T module port are related to the Ethernet 10Base-T module LEDs indication, which determines the relevant actions you need to take to troubleshoot the router.

Table 28: Ethernet 10Base-T Module LEDs

LED	Description	Indication	Status and Troubleshooting Action
Link	Indicates whether the link is established.	Green	The link is established. No action is necessary.
		OFF	The link is not established. **1** Using UEM, check the conditions and alarms for the router. Also, check the router configuration and router log information in UNC. Lastly, check the alarms and configuration for the device on the other end of the link.

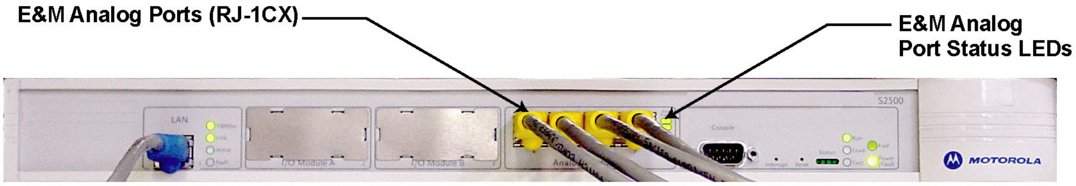
LED	Description	Indication	Status and Troubleshooting Action
			2 Verify the configuration for the router in the UNC. If applicable, send an enable diagnostic command for the router through UEM. **3** Check the physical connection to the port. Verify that the cable is properly connected and in good condition. **4** Try to reboot the router through UNC, or cycle power to the router. **5** If the port fails to establish a connection, power down the router and test the cable for problems, as possible. Replace the cable if necessary. **6** If the port still fails, try to reload the EOS and configuration files to the router through UNC. **7** If the router still fails to operate properly, replace the router.
Transmit	Indicates that a packet has been transmitted.	Flickering Green	The port is sending traffic normally. No action is necessary.
		OFF	No activity is detected. If the port should be active, troubleshoot the router as explained for a Link LED failure above.
Receive	Indicates that a packet has been received.	Flickering Green	The port is receiving traffic normally. No action is necessary.
		OFF	No activity is detected. If the port should be active, troubleshoot the router as explained for a Link LED failure above.
Collision	Indicates that a fault has been detected.	OFF	The port is okay. No action is necessary.
		Amber	A fault has been detected. The network needs to be checked for speed/duplex mismatches and for any loops that may have been created in error.

2.7.8
E&M Module LEDs Troubleshooting

The fault conditions of the E&M module are related with the E&M module LEDs indication, which determines the relevant actions you need to take to troubleshoot the router.

The Port Status LEDs (one per E&M port) indicate the status of the analog conventional channel associated with the E&M port.

Figure 24: E&M Port LEDs



S2500Router_wCCGW_front_wCallouts

Table 29: E&M Module LEDs

Indication	Status and Troubleshooting Action
Steady Green	The analog channel corresponding to this port is enabled and idle. No action is necessary.
Blinking Green	The analog channel corresponding to this port is enabled, and audio packets are flowing. No action is necessary.
Yellow	CCGW functionality is not enabled; the DSP is out of service; or a fault has been detected on the analog channel corresponding to this port. **NOTICE:** When the S2500 boots up, the E&M port LEDs are yellow until the first analog channel is configured. Once an analog channel is configured, the E&M port LEDs are off and turn yellow if an enabled/ active channel fails. **1** Using UNC, check the router configuration and verify that the CCGW service CONTrol parameter is set to Enable. **2** Check the LDAP server configuration and verify that the site type is configured as analog.
OFF	CCGW functionality is enabled, but the channel corresponding to this port is disabled or is not configured to use an E&M port (for example, it is a V.24 digital channel). **1** Using UNC, check the router configuration and verify that the CCGW service CHControl parameter is set to **Enable** for this port. Also, check the alarms and configuration for the device on the other end of the link. **2** Check the LDAP server configuration and verify that an analog conventional channel has been created for this port. **3** Make sure that the DSP SIMM is installed properly.

2.7.9
V.24 Module LEDs Troubleshooting

The fault conditions of the V.24 module are related with the V.24 module LEDs indication, which determines the relevant actions you need to take to troubleshoot the router.

The Port Status LEDs (one per V.24 port) indicate the status of the ASTRO® 25 system Conventional channel associated with the V.24 port.

Figure 25: V.24 Module LEDs

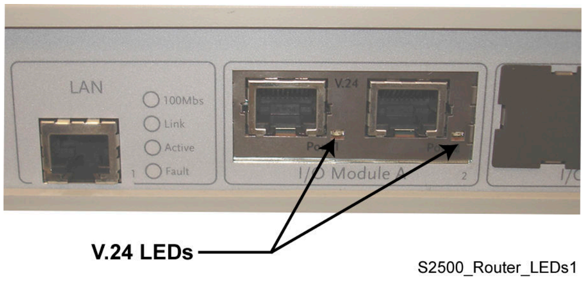


Table 30: V.24 Module LEDs

Indication	Status and Troubleshooting Action
Solid Green	The V.24 port is connected, the HDLC link is up, and the ASTRO® 25 Conventional channel corresponding to this port is enabled and idle. No action is necessary.
Blinking Green	The V.24 port is connected, the HDLC link is up, the ASTRO® 25 Conventional channel corresponding to this port is enabled, and audio packets are flowing. No action is necessary.
Yellow	The CCGW service is enabled and the corresponding channel is configured to use the V.24 port (it is a digital channel), but the V.24 port is not connected. **1** Using UEM, check the conditions and alarms for the router. Also, check the status of the base radio or LAN to which the V.24 port is connected. **2** Check the physical connection to the V.24 port and verify that the cable is connected and in good condition.
Off	The CCGW service is disabled or the corresponding channel is not configured to use the V.24 port (it is an analog channel). **1** Using UNC, check the router configuration and verify that the CCGW service CHControl parameter is set to **Enable**. **2** Using UNC, check the router configuration and verify that the CCGW service CHControl parameter is set to **Enable** for this port.

2.7.10 Troubleshooting Routers in the Unified Network Configurator (UNC)

The Unified Network Configurator (UNC) uses VoyenceControl to configure and monitor the status of the routers. Using the router management function, the configurations are viewed, created, and modified using templates. For the step-by-step procedures, refer to the “UNC Operation” chapter of the *Unified Network Configurator* manual.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.
This topic does not apply to unmanaged routers – the Border Router and Peripheral Network Routers or if the system is supported by a K core.

2.7.11 Troubleshooting Traps in the Unified Event Manager (UEM)

Alarms and traps generated by routers are sent to the Unified Event Manager (UEM) server located in the same zone as the site in which the router is located. The remote site router must be discovered in the UEM application using subnet discovery before traps are visible in UEM.

Router faults, events, alarms, and link up/down status are reported in the UEM application. For additional information on subnet discovery as well as a list of router alarms and traps and their definitions, refer to the *Unified Event Manager Online Help*.

NOTICE: This topic does not apply to unmanaged routers – the Border Router and Peripheral Network Routers.

2.8 S2500 FRU/FRE Procedures

This section lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs), and includes replacement procedures applicable to the routers.

2.8.1 Tools and Equipment Required for Router Replacement

Specific tools and equipment are required during the router replacement at the site.

Take the following items to the site when replacing the routers:

- Electrostatic Discharge (ESD) strap (Motorola Solutions part number RSX4015A, or equivalent)
- Laptop PC with a 3Com Trivial File Transfer Protocol (TFTP) server software and a terminal emulation program such as HyperTerminal or ProComm+ installed
- Ethernet crossover cable
- DB9 null modem cable
- Crosstip and slotted screwdrivers
- Set of TORX drivers

2.8.2 Shipping Carton Content

When you receive the router, verify that the carton includes the following items:

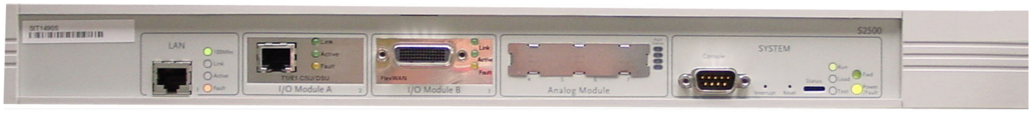
- Router configured with I/O modules based on router function
- Power cable
- Rack-mount kit
- EOS Software and User Documentation media device

  NOTICE: The software is pre-installed in the flash memory drive of the router and automatically loads when you turn on the power. Software provided on a media device is for software recovery purpose only.
- Release notes
- License agreement

2.8.3 Field Replaceable Entity – S2500

The following figure shows an example remote site router Field Replaceable Entity (FRE).

Figure 26: S2500 Field Replaceable Entity



S2500_router

The table lists the base router along with its part number. Use the part number for the item when ordering.

Table 31: S2500 Router Field Replaceable Entity

Component Type	Where Used	Part Number
S2500 router	Control Room Site Remote Network Management/Remote Console Client	ST2500 or ST2500B

NOTICE: Version B (or higher) features a new version of the Programmable Logic Device (PLD)

2.8.4
Replacing a Router – S2500

Replace a router by removing the existing router, installing and configuring the replacement router.

Prerequisites: Verify that you have access to the appropriate router configuration files for the router you are replacing. You can find the files on the media device containing the electronic version of the system-specific configuration documentation provided by Motorola Solutions. If you do not have access to the media device, contact your system administrator.
Wear an Electrostatic Discharge (ESD) strap and connect its cable to a verified good ground.

See Configuration Prerequisites on page 35 for all necessary prerequisites

CAUTION: The Electrostatic Discharge (ESD) strap must be worn throughout the whole procedure to prevent ESD damage to any components.

NOTICE: If redundant site links are supported, powering down an active site router causes the redundant site router to route the full load of traffic for the site, and communication is not affected. However, if redundant site links are not supported, powering down the site router causes the repeater site to enter site trunking mode until the router is operational again.

IMPORTANT:
Before replacing the router, pull configuration and hardware information from the router into the Unified Network Configurator (UNC) by performing the Pull All operation. See the “Scheduling the Pull of Device Configurations” procedure, in the *Unified Network Configurator* manual.

The Pull All operation is not possible if communication is severed between the router and UNC, if the router is not managed by UNC, or if the system is supported by a K core. If any of these scenarios exist, perform any one of the following:

- Use the last known good configuration files from the UNC
- Extract the configuration files from the router directly
- Use the configuration files provided by Motorola Solutions when your system was commissioned. Typically, configuration files are provided on a media device as part of the Electronic Build Book.

No matter what the source of the Configuration files is, the files themselves need to be copied to the service PC with 3com TFTP software enabled.

NOTICE: If you replace a router as a unit, the replacement router must have the same hardware configuration (that is, the same I/O modules installed in the same I/O module slots.)

When and where to use: Use the following steps to replace a router when it fails to operate properly and the troubleshooting actions are unsuccessful.

IMPORTANT: Power down the router before servicing or replacing any interface modules. Powering down a router causes network services to and from the supported site to be suspended until the router is replaced and brought back into service. Wide area voice traffic and networking services should not be affected, but the traffic capacity may be reduced until the router is brought back into service.

Procedure:

1 Power down the existing router by disconnecting the power cable from the router and remove any cables that are installed on the chassis.

   DANGER: Shock hazard: Routers contain dangerous voltages, which can cause electrical shock or damage to equipment. Turn off the router and remove the power cabling when servicing this equipment.

2 Remove the existing router:

   a Label and disconnect all communication cabling from the router.

   b Disconnect the ground cable from the rear of the chassis.

   c Remove the screws securing the router to the rack.

   d Pull out the router through the front of the rack.

3 Remove the mounting brackets from the existing router and install the brackets on the replacement router.

4 Install the replacement router:

   a Install the replacement router in the rack and secure it with the screws that were previously removed.

   b Secure the ground cable to the ground location on the rear of the chassis.

   c Attach all communication cabling to the router.

5 Power up the replacement router by reconnecting the power cable to the router.

6 Configure the router according to the process in Router Configuration on page 35.

   NOTICE: When replacing a router, Completing the Configuration on page 40, step 8, which directs you to discover the router in the UNC, does **NOT** apply. Instead, perform the following steps from the process “Replacing a Device” in the *Unified Network Configurator* manual:

   a For this device, execute the **Clear USM Cache** saved command from the list of saved commands under **System**, **Motorola**, then **SNMPv3**. For instructions on accessing and executing saved commands for a device, see “Accessing and Executing Existing Saved Commands” in the *Unified Network Configurator* manual.

   b Use the test credential quick command to test the credentials. For instructions, see “Executing Quick Commands”in the *Unified Network Configurator* manual.

   c Pull the configuration for the new device. For instructions, see “Pulling the Configuration for a Single Device” in the *Unified Network Configurator* manual.

7 Compare the version of the Enterprise Operating System (EOS) software that is running on the replacement router with the version that was running on the replaced router, by running the Compare function in the hardware history in the UNC. See “Comparing Device Configuration Versions” in the *Unified Network Configurator* manual.

   NOTICE: If the replacement router needs a software update, perform the upgrade. Perform “Operating System and Software Upgrade” as described in the *Unified Network Configurator* manual.

8 Check for any differences between the configurations, and determine whether either configuration needs to be corrected.

- If the previous configuration needs to be restored, then see the “Rolling Back to a Previous Version” section in the *Unified Network Configurator* manual.
- If the current configurations are changed and sent to the router, see the “Device Update with a Download of Configuration Changes” section in the *Unified Network Configurator* manual.

Postrequisites: Verify that the replacement router is operating properly.

2.8.5 Field Replaceable Units – S2500

The base router (model ST2500) is configured with the I/O modules necessary to meet the operating requirements of each functional router. The I/O modules are Field Replaceable Units (FRUs).

The S2500 base router ships with the following:

- One Ethernet (10Base-T/100Base-TX) port
- A console (serial) port
- Two I/O slots for optional I/O modules
- One analog module slot

Port Number Assignment

The I/O modules are installed in slots labeled with port numbers 2 and 3.

- If the module is installed in I/O module slot A, the port number is 2.
- If the module is installed in I/O module slot B, the port number is 3.

The E&M module is installed in the slot labeled with port numbers 4, 5, 6 and 7.

FRUs for S2500 Routers

Table 32: FRUs for S2500 Routers

FRU Module ID	FRU Brief Description	FRU Expanded Description
ST2510	1-Port Ethernet 10Base-T module	Used when the site router supports the Flexible Ethernet Links feature. Supported in I/O slot A only.
ST2511	1-Port FlexWAN (V.35) module	Used when the router supports a circuit-based Conventional channel. The FlexWAN port connects to a High Speed Unit (HSU) module in a channel bank. Supported in I/O slots (A and B).
ST2512	1-Port T1/E1 module	Used when the router supports a prime site (master site) interface. Supported in I/O slots (A and B).
ST2514	ASTRO® 25 Digital Conventional-to-IP Interface Kit (V.24 module)	Used when the router supports an ASTRO® 25 system Conventional Digital CCGW at the site. A V.24 module adds two V.24 digital interface ports. Supported in I/O slots (A and B).
ST2513	ASTRO® 25 Analog Conventional-to-IP Interface Kit (includes E&M module and DSP SIMM)	Used when the router supports Analog conventional channels at the site (Analog CCGW). A hardware kit adds four 4-Wire interface ports to CCGW. Supported in the analog module slot.

FRU Module ID	FRU Brief Description	FRU Expanded Description
		NOTICE: Requires an MNR S2500 base unit model number ST2500B (part number CLN1713B or later). If you install the Analog Conventional-to-IP Interface Kit in a router at a previous hardware revision level, it does not function.

Table 33: FRUs by Router Usage

S2500 Router	ST2510	ST2511	ST2512	ST2514	ST2513
	10Base-T	FlexWAN	T1/E1	V.24	E&M
Circuit Simulcast Remote Site Router	N/A	X	X	X	X
IP Simulcast Remote Site Router	X	X	X	X	X
ASTRO 25 Repeater Site Router	X	X	X	X	X
HPD Remote Site Router	X	X	X	X	X
ISSI.1 Site Router	X	X	X	N/A	N/A
Dispatch Console Site Router	X	N/A	X	X	X
Conventional RF Site Router	X	X	X	X	X
Analog Conventional Channel Gateway (CCGW)	N/A	N/A	N/A	N/A	X
Digital CCGW	N/A	N/A	N/A	X	N/A

2.8.6

Replacing an Optional I/O Module – S2500

Replacing an optional I/O module in the S2500 chassis consists of removing the cover of the chassis, exchanging the modules and then replacing the cover. Before performing this task, certain precautions need to be completed.

Prerequisites: Familiarize yourself with the Electrostatic Discharge (ESD) precautions.

CAUTION: ESD PRECAUTIONS
When removing or installing modules, take the following precautions to prevent Electrostatic Discharge (ESD) from damaging the internal components of the router:

- Always wear a properly grounded Electrostatic Discharge (ESD) wrist strap.
- Transport static-sensitive components in anti-static packaging.
- Keep static-sensitive components in their anti-static packaging until you are ready to install them.
- Just before removing components from their anti-static packaging, discharge static electricity from your body by touching an unpainted metal surface.
- When you handle modules, place them with the printed circuit side down on a nonconducting, static-free, and flat surface.

When and where to use: Use the following steps to replace the I/O module when it fails to operate properly or you are replacing an S2500 router as a unit.

IMPORTANT: Do not store unused or unconfigured I/O modules in unused router slots.
If you remove an S2500 I/O module, you must replace it with a module of the same type. For example, if you remove a FlexWAN module, you must replace it with another FlexWAN module, not a T1/E1 module. Similarly, if you replace an S2500 router as a unit, the replacement router must have the same hardware configuration (that is, the same I/O modules installed in the same I/O module slots).

The Analog Conventional-to-IP Interface Kit requires an MNR S2500 base unit model number ST2500B (part number CLN1713B or later). The base unit model number and part number are listed on the rear of the router. If you install the Analog Conventional-to-IP Interface Kit in a router at a previous hardware revision level, it does not function.

NOTICE: For the list of optional modules, see Field Replaceable Units – S2500 on page 104.
If the MNR S2500 is configured for use in a secure (Common Criteria) environment, the device is equipped with tamper evidence labels, which will be broken if you perform the following procedure. Contact Motorola Solutions to order replacement labels (part number TYN4008A), and follow the instructions provided with the labels to reapply them.

The example shown in this procedure applies to the ST2513, the Analog Conventional-to-IP Interface Kit (E&M module and DSP SIMM).

Procedure:

1 Power down the existing router by disconnecting the power cable from the router and remove any cables that may be installed on the chassis.

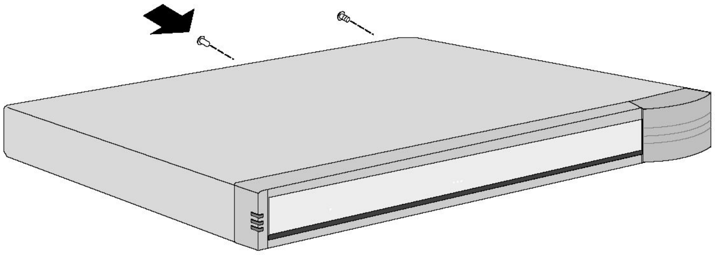
DANGER: Shock hazard: Routers contain dangerous voltages, which can cause electrical shock or damage to equipment. Turn off the router and disconnect the power cabling when servicing this equipment. Always disconnect the power cabling before removing the router cover.

2 Remove the cover from the S2500 chassis.

a If mounting brackets are present, remove them from the chassis.

b Remove the two screws that secure the cover to the chassis on the rear of the router.

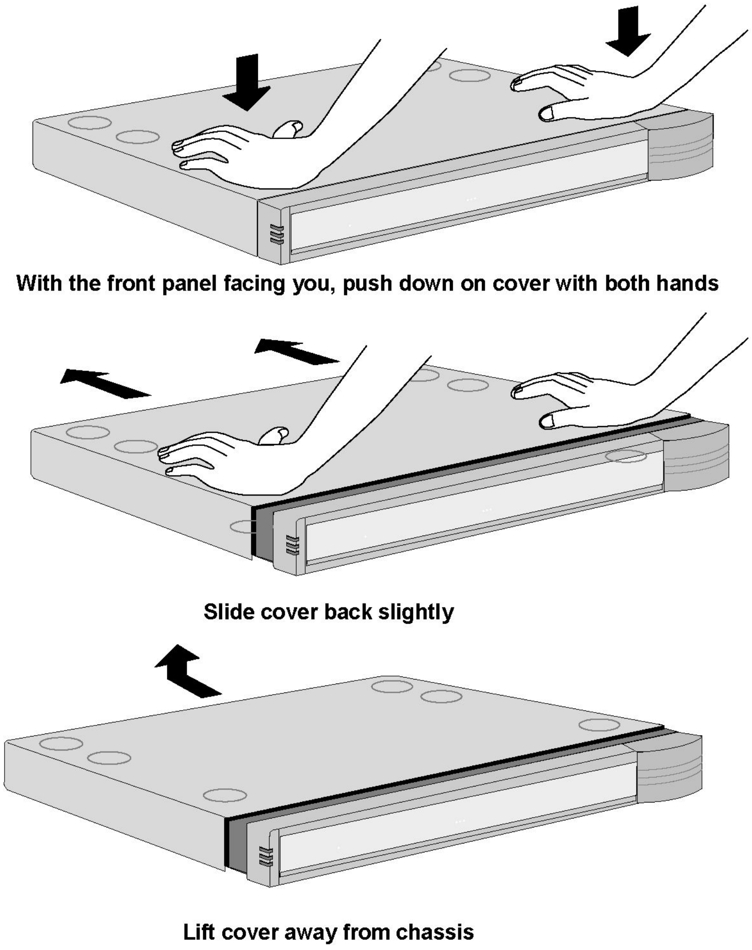
Figure 27: Removing the Screws that Secure the Chassis



S2500_cover_replacement

c Remove the cover from the chassis.

Figure 28: Removing the Cover from the Chassis



With the front panel facing you, push down on cover with both hands

Slide cover back slightly

Lift cover away from chassis

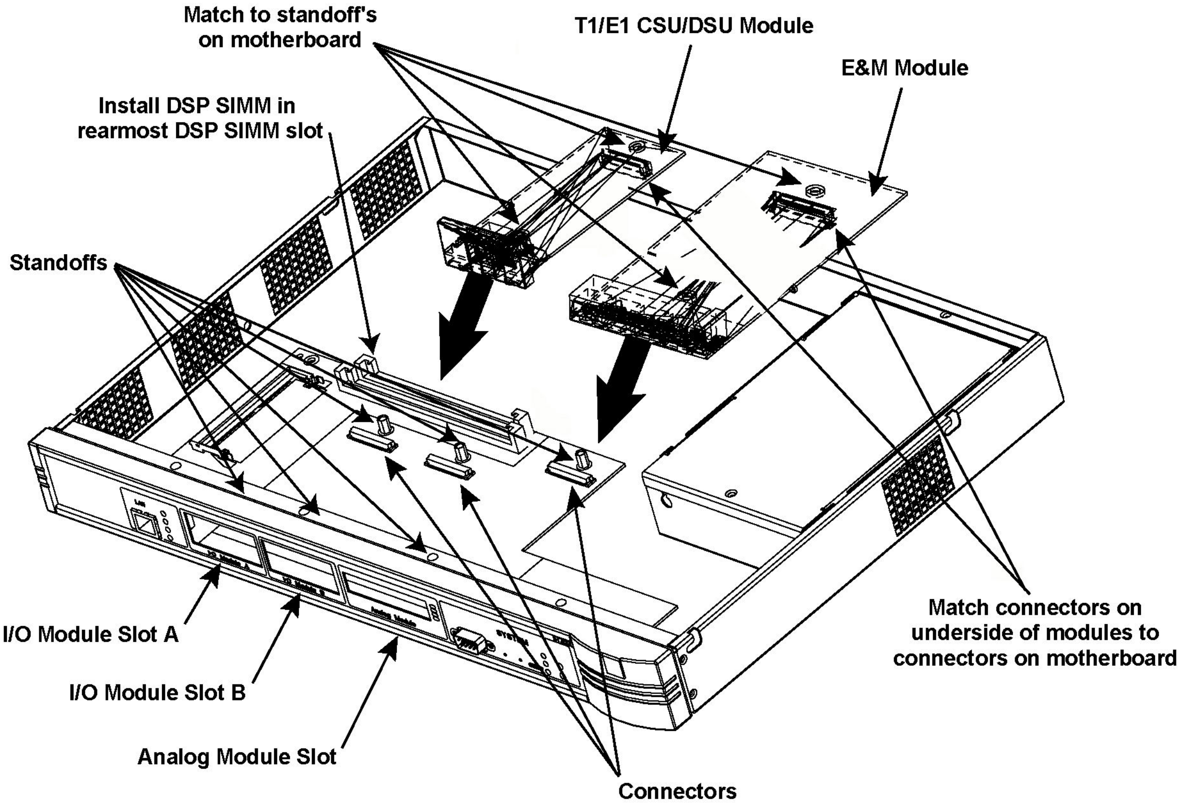
S2500_optional_module_install

3 Remove the existing module.

a Locate the module you want to replace and remove the screws from the standoff. Set the screws aside, as you need them later in this procedure.

b Gently remove the module from the connector pins by pulling the connector up and off.

Figure 29: I/O Module Slot, Connector, and Standoff Locations on the Router Motherboard


Match to standoff's on motherboard
T1/E1 CSU/DSU Module
E&M Module
Install DSP SIMM in rearmost DSP SIMM slot
Standoffs
I/O Module Slot A
I/O Module Slot B
Analog Module Slot
Connectors
Match connectors on underside of modules to connectors on motherboard

S2500_motherboard

4 If you install or replace DSP SIMM , perform the following actions:

- a Locate the rearmost DSP SIMM that is installed in the rearmost DSP SIMM slot, and remove this slot.
- b Insert the new DSP SIMM into the slot at a 30 degree angle, with the SIMM angled forward (toward the front of the chassis).
- c Press back on the SIMM to seat it into position.

  The socket clips automatically engage the SIMM as you move it into position.

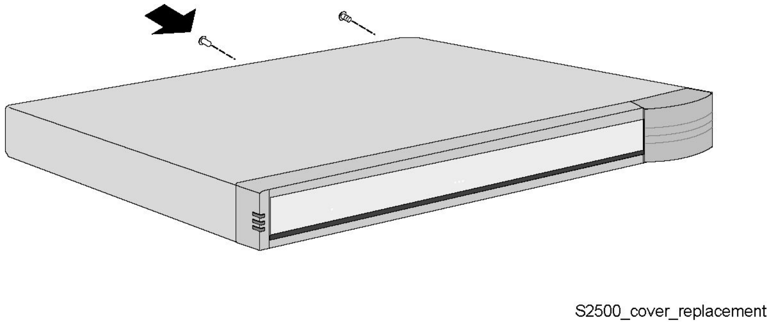
5 Insert the new module.

- a Coming from the back of the chassis, insert the front of the module through the front panel of the chassis.
- b Line up the connector pins carefully.
- c Press down gently on the module.

6 Secure the module with the two screws you removed in step 3. To ensure that the module is seated properly, tighten the screws securely.

7 Replace the cover and secure it to the chassis with the two screws you removed in step 2.

Figure 30: Replacing the Cover on the Router Chassis



Postrequisites: Power up the router and verify that the replaced module is working properly.

Chapter 3

ASTRO 25 Master Site

This chapter provides information on the routers in an ASTRO® 25 system master site.

NOTICE: The GGM 8000 can be used as a replacement for the following S6000 routers employing Ethernet site links: S6000 GGSN (GPRS Gateway Support Node), S6000 Gateway Router, S6000 Core Router, and S6000 Exit Router. See the *System Gateways – GGM 8000* manual for details.

3.1 Master Site Routers – Functional Description

This chapter explains how the S6000 master site routers work in the context of your system.

If a Dynamic System Resilience (DSR) configuration is implemented on your system, see the *Dynamic System Resilience* manual for details. Dynamic System Resilience allows a system to continue to operate without loss of function on the failure or destruction of any controlling master site within a single or multizone by providing geographically redundant Fixed Network Equipment.

3.1.1 Master Site Routers – Network Connections

Various master site routers (S6000 platform) are included in the zone core to support network transport connectivity.

The number of network transport devices and the type of devices depends primarily on the size of the system, the type of zone core configuration, and the data services available. The following are various types of routers commonly found in a zone core to support network transport connectivity:

Core Router – M and L zone cores
Supports Intra-Zone traffic (zone-to-site traffic).

Exit Router – M3 zone core
Supports Inter-Zone traffic (zone-to-zone traffic, multi-zone systems).

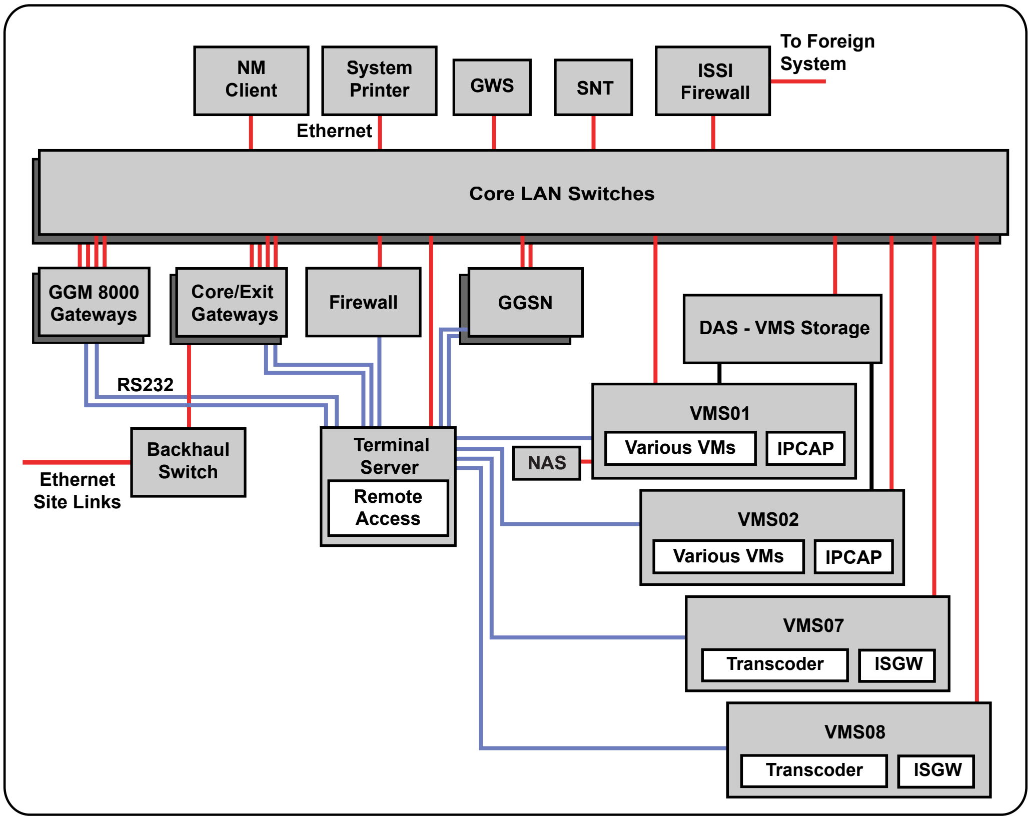
Core/Exit Router – M1 and M3 zone cores
Dual function transport device providing Intra-Zone and Inter-Zone support.

Gateway Router – M and L zone cores
Supports network traffic between various subnets within the zone core.

GGSN Router – M and L zone cores
Supports network traffic between the RNI and CEN for packet data applications.

The following figure provides an example of a master site for an M3 zone configuration showing separate Core and Exit routers deployed with the Cooperative WAN Routing Relay Panels to support T1/E1 site links.

Figure 31: Master Site Routers – T1/E1 Site Links

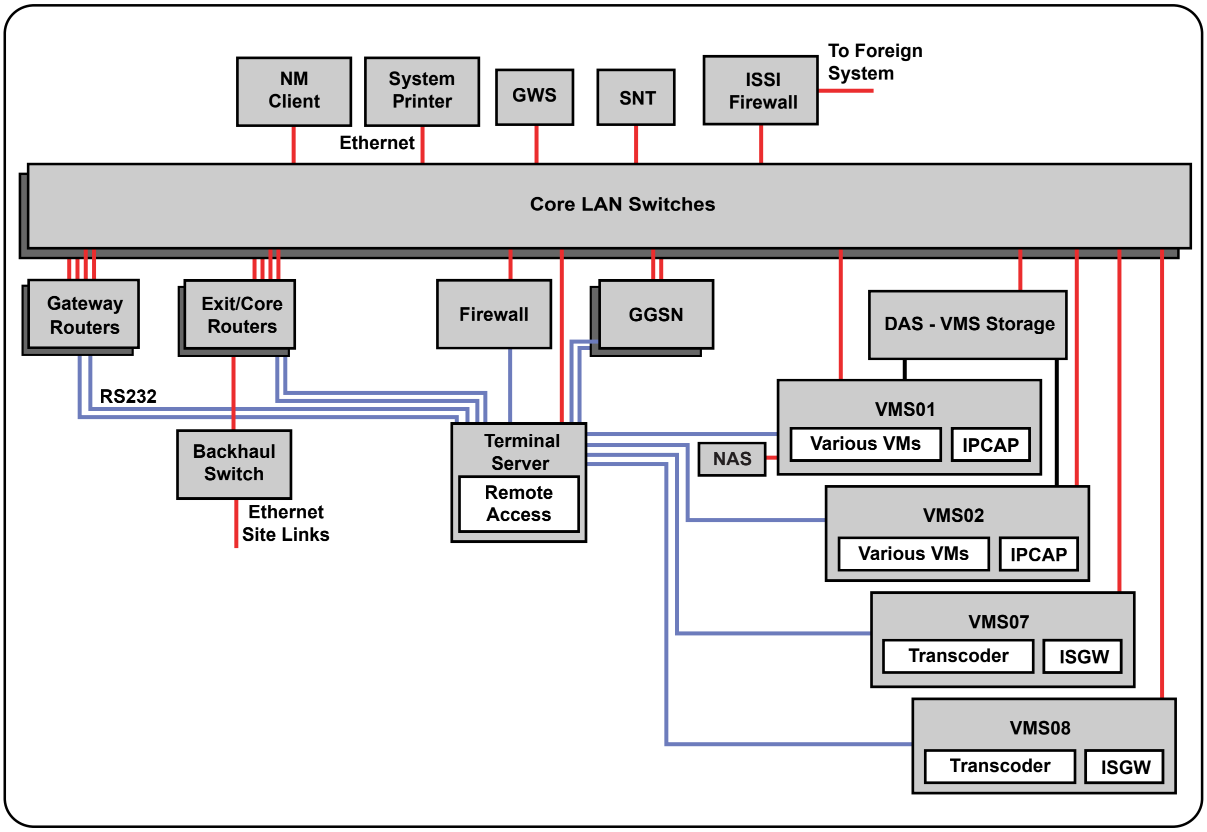


S_A717_M3_Primary_System_Zone_Core_Config_A

NOTICE: The master site for an M3 zone core configuration can implement Ethernet site links by employing a dual-function Core/Exit Router or separate Core and Exit routers. For more additional zone core architecture diagrams, see the *Master Site Infrastructure Reference Guide* manual.

The following figure provides an example of a master site for an M3 zone core configuration showing the dual-function Core/Exit routers deployed with Ethernet site links.

Figure 32: Master Site Routers with Dual-Function Core/Exit Routers – Ethernet Site Links



S_A717_M3_Core_Exit_Dual_Function_Zone_Core_Config_B

NOTICE: For more details and information on an Ethernet site link implementation at the master site featuring core backhaul LAN switches, see the *Flexible Site and InterZone Links* manual.

3.1.2

I/O Modules Required for Master Site Routers

The I/O modules for master site routers in the ASTRO® 25 system are installed in certain slots.

Table 34: Master Site Routers – I/O Modules Required

Functional Router Description	S6000 I/O Slot 1 Port 4	S6000 I/O Slot 2 Port 5
Core router	ST6015 or ST6018	ST6015 or ST6018
Exit router	ST6015 or ST6018	ST6015 or ST6018
Core/Exit router	Empty	Empty
Gateway router	Empty	Empty
GGSN router	Empty	Empty
Border router	As needed	As needed
Peripheral Network Router	As needed	As needed

For more information about the Border router and Peripheral Network Router, see ASTRO 25 Customer Enterprise Network on page 200.

3.1.3 Enterprise Operating System Functions

The S6000 router uses basic routing and IP features in the Enterprise OS (EOS) software including the following:

- IP Routing
- 10/100 Ethernet
- E1/T1 channelized
- E1/T1 unchannelized
- Static Routes
- Frame Relay
- Fragmentation

The S6000 router uses the following protocols and interfaces:

- Point to Point Protocol (PPP)
- Simple Network Management Protocol (SNMP)
- Type of Service (TOS)
- Network Time Protocol (NTP)
- Multicast

NOTICE: Network transport devices (routers, switches, firewalls and others) are pre-configured to support systems with and without a TRAK 9100 NTP Server, so the primary NTP Server is set to ntp02, which is always present in the system. For details regarding the Network Time Protocol (NTP) Server, as well as the primary and secondary NTP source for devices in your system, refer to the *Network Time Protocol Server* manual.

3.2 Master Site Routers – Installation and Configuration

Prerequisites: Ensure that you have the required cabling and connectors.

Process:

1. Install the Master Site Router in a rack. See S6000 Introduction, Installation, and Configuration on page 27.
2. Connect the Master Site Router to a power source. See S6000 Introduction, Installation, and Configuration on page 27.
3. If necessary, ground the Master Site Router. See S6000 Introduction, Installation, and Configuration on page 27.
4. Connect the equipment to the Master Site Router. For Master Site Router cable connections, see the *Master Site Infrastructure Reference Guide* manual. For the GGSN router, see GGSN Router – Site-Specific Cabling on page 129.
5. Configure the Master Site Router. See S6000 Introduction, Installation, and Configuration on page 27.

3.3 Master Site Routers – Maintenance and Troubleshooting

Generic maintenance and troubleshooting procedures apply. For maintenance and troubleshooting information, see S6000 Introduction, Installation, and Configuration on page 27.

3.3.1 Master Site Routers – General Troubleshooting

This section discusses troubleshooting steps for general problems with the S6000 routers.

NOTICE: See the *Flexible Site and InterZone Links* manual for troubleshooting information relating to Ethernet LAN links.
In systems with a Dynamic System Resilience (DSR) configuration installed, there is one more level of redundancy for network transport routers, resulting in a lower number of connectivity problems and less troubleshooting required. For more information on a Dynamic System Resilience configuration, see the *Dynamic System Resilience Feature Guide* manual.

3.3.2 Master Site Router – CWR Troubleshooting

This section describes the hardware failures in Cooperative WAN Routing (CWR).

The CWR solution provides a mechanism for redundant pairs of core and exit routers to directly failover non-redundant T1/E1 links between the router pair.

For replacing an S6000 router implemented as a CWR peer, see Replacing a Router – S6000 on page 60.

3.3.2.1 Relay Panel Failure

The relays are latching and retain their last state during power failures, or loss of communications with the core and exit routers. There is no loss of connectivity.

3.3.2.2 Master Site Router Failure

Each S6000 core router contains up to 24 T1/E1 ports. The routers are deployed in pairs as Active and Inactive.

The core router failures are as follows:

- The connection between the Active router and the relay panel fails. The router hardware detects this failure. Once it is detected, a signal is sent to the relay to switch all associated ports to the Inactive router.
- Individual site or InterZone links fail. These failures do not cause switching between the routers.
- The Active router fails completely. This is detected by the Inactive router through the communication between the two routers. Once the failure is detected, the Inactive router switches all the relays to itself, and becomes the Active router.
- In the event of a total damage of the relay panel, it is possible to lose all the sites connected to the panel. However, power failures and communication failures to the panel leave all the site links connected to one of the core routers.

3.3.2.3 Cooperative WAN Routing Troubleshooting Tools

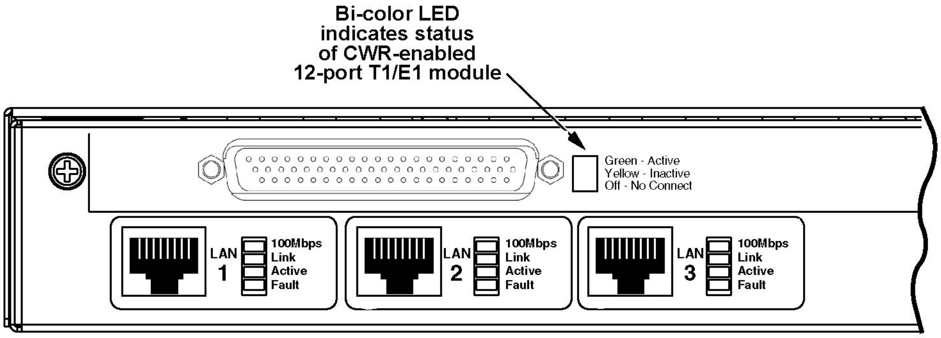
The tools used for troubleshooting CWR are as follows:

- Unified Event Manager
- Unified Network Configurator
- InfoVista
- Local Router Administration

3.3.2.4 12-Port T1/E1 (CWR) Module LED

The 12-port T1/E1 module features a single bi-color LED. The LED indicates CWR status of the module.

Figure 33: 12-Port T1/E1 (CWR) Module LED



CWR_12port_T1E1_module_LED

Table 35: 12-Port T1/E1 (CWR) Module LED

LED	Indication	Status and Troubleshooting Action
Bi-color LED	Green	The module is connected to the relay panel and is functioning as the active CWR peer.
	Amber	The module is connected to the relay panel and is functioning as the inactive CWR peer.
	OFF	The module is not connected to the relay panel.

3.4 Gateway Router (M and L Zone Cores)

The gateway router provides functional support for the zone controller, packet data gateway (PDG), and network management system routing.

NOTICE: The GGM 8000 can be used as a replacement for S6000 Gateway Routers employing Ethernet site links. See the *GGM 8000 System Gateway* manual for details.

3.4.1 Gateway Router – Functional Description

The gateway router serves as the single access interface for all information intended for the zone controller and the Packet Data Gateway (PDG). Any traffic to and from these devices is routed through the gateway router.

A gateway router functions as data and control router, and its functions include:

- Providing an audio switch interface and network management functionality
- Providing a level of isolation for the zone controller and the PDG
- Supporting multicast traffic, allowing the zone controller to send control packets to multiple points in the zone

Two gateway routers are installed on the Local Area Network (LAN). The gateway router is a Motorola Network Router (MNR) S6000 with an ST6011 module in I/O slot 1.

Gateway routers are used for devices that require network redundancy and are multicasting beyond their local LAN. Gateway routers provide support for the following:

- Zone Controller (control router functionality)
- Packet Data Gateway (PDG router functionality)
- Network Management

Gateway routers provide several benefits for the zone's master site:

- Provide a single access point or gateway to access the core and exit routers.
- Isolate multicast traffic from the various hosts they are servicing.
- Provide redundant connections for hosts with redundant interfaces (zone controller) because there are two for each function.

Each gateway router has two 100Base-TX connections to one of the master site LAN switches. One router connects to TLAN 1 and the other connects to TLAN 2. Any traffic to and from the zone controllers or the PDG is routed by one of the gateway routers. Each gateway router has an RS232 connection to the terminal server, allowing router administration by PC clients over the LAN.

NOTICE: See the *Dynamic System Resilience Feature Guide* manual for additional configurations.

See Master Site Routers – Network Connections on page 110 for a network transport diagram showing the gateway router.

3.4.2 Gateway Router – Installation and Configuration

Prerequisites: Ensure that you have the required cabling and connectors.

Process:

1. Install the Gateway Router in a rack. See S6000 Introduction, Installation, and Configuration on page 27.
2. Connect the Gateway Router to a power source. See S6000 Introduction, Installation, and Configuration on page 27.
3. If necessary, ground the Gateway Router. See S6000 Introduction, Installation, and Configuration on page 27.
4. Connect the equipment to the Gateway Router. For gateway router cable connections. See Gateway Router – Site-Specific Cabling on page 116.

   Gateway routers connect directly to the Zone Core LAN switches (Master Site LAN switches) to support the functional network requirements of the other master site components.
5. Configure the Gateway Router. See S6000 Introduction, Installation, and Configuration on page 27.

3.4.2.1 Gateway Router – Site-Specific Cabling

The following table lists the Gateway router port assignments when used in an M or L zone core configuration.

Table 36: Gateway Router Cabling – M1 or L1 Zone Core Configuration

Gateway Router	Port	Device/Port/VLAN
Gateway Router 1	LAN 1	Core LAN Switch 1 / Port 1 / QTAG

Gateway Router	Port	Device/Port/VLAN
	LAN 2	Core LAN Switch 1 / Port 2 / TLAN 1
	RS-232	Terminal Server or Local Serial Access

Table 37: Gateway Router Cabling – M2, M3,or L2 Zone Core Configuration

Gateway Router	Port	Device/Port/VLAN
Gateway Router 1	LAN 1	Core LAN Switch 1 / Port 1 / QTAG
	LAN 2	Core LAN Switch 2 / Port 3 / TLAN 1
	RS-232	Terminal Server or Local Serial Access
Gateway Router 2	LAN 1	Core LAN Switch 1 / Port 1 / QTAG
	LAN 2	Core LAN Switch 2 / Port 3 / TLAN 2
	RS-232	Terminal Server or Local Serial Access

3.4.3 Gateway Router – Maintenance and Troubleshooting

Generic maintenance and troubleshooting procedures apply. For maintenance and troubleshooting information, see S6000 Introduction, Installation, and Configuration on page 27.

3.5 Core/Exit Router (M1 and M3 Zone Cores)

Depending on performance and capacity requirements and considerations for the zone core, a single router transport device may be deployed as a single-function device or dual-function device.

3.5.1 Core/Exit Router – Functional Description

The Core/Exit router (S6000 platform in a multi-zone system) may be deployed as a dual-function transport (gateway) device for Intra-Zone (zone-to-site) network traffic (Core router) and Inter-Zone (zone-to-zone) network traffic (Exit router).

If T1/E1 site links are used to support intra-zone traffic (Core router function) or if T1/E1 site links are used to support inter-zone traffic (Exit router function) separate Core and Exit router devices are required.

For details regarding the single-function Core router and Exit router and their functions, see the following:

- Core Router (M and L Zone Cores) on page 119
- Exit Router (M3 Zone Core) on page 123

3.5.1.1 Core/Exit Router – Network Connections (Master Site)

Each core/exit router also has an RS-232 connection to the terminal server, allowing router administration by PC clients over the LAN.

See Master Site Routers – Network Connections on page 110 for a network transport diagram showing the core/exit router.

For information on core/exit router cabling, refer to the customized configuration information provided by Motorola Solutions for your system.

NOTICE: See the *Dynamic System Resilience Feature Guide* manual for additional configurations.

3.5.1.2
Core/Exit Router to Site Connectivity

The Core/Exit router is used for site link connectivity and it interfaces directly to the zone core LAN switch and Backhaul switch at the master site to provide an Ethernet interface to the sites in the zone.

The Core/Exit router only supports an Ethernet interface (no T1/E1 links allowed) in multi-zone systems. For details regarding Ethernet site links, see the *Flexible Site and InterZone Links* manual.

3.5.2
Core/Exit Router – Installation and Configuration

Prerequisites: Prepare the required cabling and connectors.

When and where to use: When you install and configure the router, cable to the Master Site Local Area Network (LAN) Switch and to the backhaul switch

Process:

1. Install the core/exit router in a rack. See S6000 Introduction, Installation, and Configuration on page 27.
2. Connect the core/exit router to the power source. See S6000 Introduction, Installation, and Configuration on page 27.
3. If necessary, ground the core/exit router. See S6000 Introduction, Installation, and Configuration on page 27.
4. Connect the core/exit router to the master site LAN switch. See Core/Exit Router – Site-Specific Cabling on page 118.
5. Connect the core/exit router to the backhaul switch. See Cabling the Core/Exit Router to the Core Backhaul Switch on page 119.
6. Configure the core/exit router. See S6000 Introduction, Installation, and Configuration on page 27.

3.5.2.1
Core/Exit Router – Site-Specific Cabling

Connect core/exit routers to master site LAN switches in an odd-even configuration. The following tables list Core/Exit Router port assignments when used in M1 and M3 zone core configurations.

Table 38: Core/Exit Router Cabling – M1 Zone Core Configuration

Core/Exit Router	Port	Device
Core/Exit Router 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 1
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access

Table 39: Core/Exit Router Cabling – M3 Zone Core Configuration

Core/Exit Router	Port	Device
Core/Exit Router 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access
Core/Exit Router 2	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access

3.5.2.2
Cabling the Core/Exit Router to the Core Backhaul Switch

If Ethernet site links are implemented to one or more sites, the third Ethernet port on each core/exit routers is connected to two core backhaul switches. They provide the link through the Ethernet backbone to the sites.

3.5.3
Core/Exit Router – Maintenance and Troubleshooting

Generic maintenance and troubleshooting procedures apply. For maintenance and troubleshooting information, see S6000 Introduction, Installation, and Configuration on page 27.

3.5.3.1
Core/Exit Router Failures

Depending on the configuration, a core/exit router failure can have different connotations:

- In an M1 configuration, if a failure of the core/exit router occurs, the local devices within a zone are no longer able to communicate with each other and Local Area Network (LAN) traffic to other zones is lost. Both intraZone and InterZone traffic stops.
- In an M3 configuration, if a a failure of one core/exit router occurs, the redundant router takes over.
- In an M3 configuration, if a failure of both core/exit routers occur, or are powered down, the local devices within a zone are no longer able to communicate with each other and Local Area Network (LAN) traffic to other zones is lost. Both intraZone and InterZone traffic stops.

Core/Exit router failures are reported in the fault management application and additional router details are available through the Unified Network Configurator (UNC) application. If a router hardware failure is suspected, perform the appropriate field replaceable entity (FRE) replacement procedures.

3.6
Core Router (M and L Zone Cores)

The core router handles network traffic between the master site and sites associated with that master site (intrazone support only).

NOTICE: The GGM 8000 can be used as a replacement for S6000 Core routers employing Ethernet site links. See the *System Gateways – GGM 8000* manual for details.

3.6.1 Core Router – Functional Description

The S6000 core routers route traffic between the master site and remote sites. The core router connects to the LAN switch on two 100Base-TX links. A core router connects to site links through the RJ45 connectors on the Cooperative WAN Routing (CWR) panel, if one is used.

The core routers used by the system are Motorola Network Router (MNR) S6000 routers configured with 12-port T1/E1 modules.

The core router performs the following tasks:

- Controls data, and network traffic in and out of the master site
- Provides control path redundancy and segregates the network management traffic
- Provides necessary services to the sites
- Provides a proactive fault management system, notifying whenever a redundant core router takes control
- Handles network traffic between the master site and remote sites within a zone (intrazone traffic)
- Provides an interface (through Ethernet Backhaul Switches) to the Primary Prime Site and Secondary Prime Site to support a Geographically Redundant Prime Site configuration.
- Can be configured to support Ethernet Site Link Statistics for the Intra-Prime Site link between the Zone Core and Prime Sites to support a Geographically Redundant Prime Site configuration. See the *Flexible Site and InterZone Links* manual for “Ethernet Site Link Statistics – Transport Devices”.

NOTICE: The core router interfaces with the Network Management server using Simple Network Management Protocol (SNMP). Network transport devices (routers, switches, firewalls, and others) are pre-configured to support systems with and without a TRAK 9100 NTP Server, so the primary NTP Server is set to ntp02, which is always present in the system. For details regarding the Network Time Protocol (NTP) Server and the primary and secondary NTP source for devices in your system, see the *Network Time Protocol Server* manual.

If Ethernet connectivity is implemented, the third Ethernet port on the router is used to make the connection to two core backhaul switches, which then link to the Ethernet backhaul network. See the *Flexible Site and InterZone Links* manual for details.

3.6.1.1 Core Router – Network Connections

Each core router has two 100Base-TX connections to separate logically defined Transitional LANs (TLANs) on separate switching modules on the LAN switch. A core router directs any traffic to other routers on the LAN, which then forward the traffic to the destination device.

A core router interfaces with remote sites through the relay panel. The relay panel serves the traffic directly to the sites, or sends the traffic through RJ-45 connectors on the T1 links to the sites.

If an ISSI.1 Network Gateway is implemented in the system, a connection between a core router and the site router of the ISSI.1 Network Gateway is established. See the *ISSI.1 Network Gateway* manual for details.

Traffic being delivered to remote sites is sent over a Permanent Virtual Circuit (PVC), which originates at the core router and terminates at the remote site router. Each PVC originates on a separate core router for redundancy, with individual PVCs setup across the core routers in a primary/secondary active/standby configuration. Most of the traffic follows its primary PVC. If there is a failure in the primary PVC, traffic switches over to the secondary PVC.

Each core router also has an RS232 connection to the terminal server, allowing router administration by PC clients over the LAN.

See Master Site Routers – Network Connections on page 110 for a network transport diagram showing the core router.

For information on core router cabling, see the customized configuration information provided by Motorola Solutions for your system.

NOTICE: See the *Dynamic System Resilience Feature Guide* manual for additional configurations.

3.6.1.2 Core Router to Site Connectivity

If T1/E1 links are implemented between sites, a core router uses the frame relay to communicate to the sites through the relay panel. There are two frame relay Permanent Virtual Circuits (PVCs) to each site, which originate at the core router, travel through the relay panel, over the T1/E1 links and ultimately terminate at the site router. The router has two Ethernet ports that connect into different layer 2 modules on the LAN switch and a 12-port T1/E1 to connect to the relay panel for intrazone.

If Ethernet links are implemented between sites, the third Ethernet port on the two core routers is used to make the connection to the two core backhaul switches installed at the master site. The switches connect to the Ethernet backbone to provide links to the sites. For details, see the *Flexible Site and InterZone Links* manual.

3.6.1.3 Hybrid Site Link Overview

The Hybrid Site Links configuration is a flexible way of connecting a redundant zone core to redundant remote sites in ASTRO® 25 systems. The Hybrid Site Links configuration allows redundant connections between the zone core and a remote site by using different connection types. Before the introduction of this configuration, the primary and redundant site links had to be of the same type, either E1/T1 or Ethernet links. This configuration enables mixing of E1/T1 and Ethernet site links, where the primary could be an E1/T1 and the secondary could be an Ethernet link, or an Ethernet link as the primary or E1/T1 as the secondary link.

Hybrid site links are available in the M2 and M3 system configurations with Dynamic System Resilience (DSR), and M3 system configuration without DSR. The Hybrid Site Links configuration connects redundant zone cores to the following remote sites:

- ASTRO® 25 Repeater Site (ISR)
- IP Simulcast Prime Site
- Network Manager/Dispatch Console Site (MCC 7500/7100 Dispatch Console only)
- Conventional-only Site (Centralized Conventional Architecture)

The hybrid links support flexible transport types by employing transport devices such as redundant GGM 8000 site gateways and S6000 core routers. The transport between a primary core router and primary site gateway, or a secondary core router and secondary site gateway within the same site must be either of the T1/E1-to-T1/E1 or Ethernet-to-Ethernet transport type. For sites that require more than one T1/E bandwidth, the Hybrid Site Links configuration supports up to two T1/E1 links bundled together.

A site gateway supports one connection type, either redundant Ethernet or T1/E1 WAN terminations. A core router can support T1/E1 terminations for some sites and Ethernet terminations for other sites.

NOTICE: The GGM 8000 replaces the MNR S6000 for all Ethernet configurations; all T1/E1 configurations require an MNR S6000.

For more information about GGM 8000 site gateway transport devices, see the *GGM 8000 System Gateway* manual.

3.6.2

Core Router – Installation and Configuration

Prerequisites: Prepare the required cabling and connectors.

When and where to use: When you install and configure the router, cable to the Master Site Local Area Network (LAN) Switch and to the relay panel.

Process:

1. Install the core router in a rack. See S6000 Introduction, Installation, and Configuration on page 27.
2. Connect the core router to the power source. See S6000 Introduction, Installation, and Configuration on page 27.
3. If necessary, ground the core router. See S6000 Introduction, Installation, and Configuration on page 27.
4. Connect the core router to the master site LAN switch. See Core Router – Site-Specific Cabling on page 122.
5. Connect the core router to the CWR relay panel or to the core backhaul switch. See Cabling the Core Router to the CWR Relay Panel on page 123 or Cabling the Core Router to the Core Backhaul Switch on page 123.
6. Configure the core router. See S6000 Introduction, Installation, and Configuration on page 27.

3.6.2.1

Core Router – Site-Specific Cabling

Connect core routers to master site LAN switches in an odd-even configuration. The following table lists Core Router port assignments when used in M and L Zone Core configurations.

Table 40: Core Router Cabling – M1/L1 Zone Core Configuration

Core Router	Port	Device/Function
Core Router 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 1
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access

Table 41: Core Router Cabling – M2/M3/L2 Zone Core Configuration

Core Router	Port	Device/Function
Core Router 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access
Core Router 2	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access

3.6.2.2 Cabling the Core Router to the CWR Relay Panel

You connect relay panel to the core router with the T1/E1 connectors through 12-port relay cables. For more information, refer to the *Cooperative WAN Routing* manual.

3.6.2.3 Cabling the Core Router to the Core Backhaul Switch

If Ethernet site links are implemented to one or more sites, the third Ethernet port on each of the two core routers is connected to two core backhaul switches. They provide the link through the Ethernet backbone to the sites.

3.6.3 Core Router – Maintenance and Troubleshooting

Generic maintenance and troubleshooting procedures apply. For maintenance and troubleshooting information, refer to S6000 Introduction, Installation, and Configuration on page 27.

3.6.3.1 Core Router Failures

Core routers are installed in pairs. Because of this redundancy, failure of one core router is transparent to the user.

- If a core router fails, the redundant router takes over.
- If both core routers fail or are powered down, local LAN devices within the zone can no longer communicate with each other. However, local devices on the master site LAN still communicate.

Core router failures are reported in the fault management application and additional router details are available through the Unified Network Configurator (UNC) application. If a router hardware failure is suspected, perform the appropriate field replaceable entity (FRE) replacement procedures.

3.7 Exit Router (M3 Zone Core)

The exit router handles network traffic between master sites (InterZone support only).

NOTICE: The GGM 8000 can be used as a replacement for S6000 Exit routers employing Ethernet site links. See the *GGM 8000 System Gateway* manual for details.

3.7.1 Exit Router – Functional Description

The S6000 exit routers function as core routers that manage traffic for the InterZone links. There are four exit routers in each zone of a multizone system. The exit routers are installed in the zone to route all inbound and outbound InterZone traffic for the zone.

The exit routers used by the system are Motorola Network Router (MNR) S6000 routers configured with 12-port T1/E1 modules.

An exit router performs the following tasks:

- Handles InterZone links. As with the core routers, exit routers have two Ethernet ports that connect into different layer 2 modules on the Local Area Network (LAN) switch and a 12-port T1/E1 connector connected to the relay panel for InterZone traffic.

  NOTICE: Exit routers use Border Gateway Protocol (BGP) for InterZone routing.

- Deploys packets among its multiple connections on both the LAN and WAN interfaces using dynamic routes. The packets destined for the control Ethernet interfaces on the zone controller, as well as the packets for network management, are routed through the Transitional LAN (TLAN) ports of the Ethernet LAN switch using dynamic routes.
- Talks to other zones through the relay panel using the T1/E1 connection. The routers learn about the Permanent Virtual Circuit (PVCs) on the T1/E1 connection from the relay panel. Each PVC originates on an exit router in one zone, and terminates on an associated exit router in the adjacent zone.

3.7.1.1 Exit Router – Network Connections

If T1/E1 links are implemented to other zones in the system, the exit router has a T1/E1 connection to the relay panel. The physical T1/E1 connection supports frame relay over a PVC, which originates at the exit router and terminates at the exit router in the other zone. Outbound InterZone traffic is sent from the LAN switch to the exit router. The exit router forwards the traffic through the relay panel to the T1/E1 connection, which in turn forwards the traffic to the other zone. The relay panel receives the outbound traffic and forwards the traffic to the other zone.

If Ethernet links are implemented to other zones, the third Ethernet port on the two exit routers is used to make the connection to the two core backhaul switches installed at the master site. The switches connect to the Ethernet backbone to provide links to the other zones. For details, refer to the *Flexible Site and InterZone Links* manual.

Each exit router has an RS232 connection to the terminal server, allowing router administration by PC clients over the LAN.

See Master Site Routers – Network Connections on page 110 for a network transport diagram showing the exit router.

NOTICE: See the *Dynamic System Resilience Feature Guide* manual for additional configurations.

3.7.2 Exit Router – Installation and Configuration

Prerequisites: Prepare the required cabling and connectors.

Process:

1 Install the exit router in a rack. See S6000 Introduction, Installation, and Configuration on page 27.

2 Connect the exit router to the power source. See S6000 Introduction, Installation, and Configuration on page 27.

3 If necessary, ground the exit router. See S6000 Introduction, Installation, and Configuration on page 27.

4 Connect the exit router to the master site LAN switch. See Exit Router – Site-Specific Cabling on page 125.

5 Connect the exit router to the CWR relay panel or to the core backhaul switch. See Cabling the Exit Router to the CWR Relay Panel on page 125 or Cabling the Exit Router to the Core Backhaul Switch on page 125.

6 Configure the exit router. See S6000 Introduction, Installation, and Configuration on page 27.

3.7.2.1 Exit Router – Site-Specific Cabling

Connect exit routers to the master site LAN switches in an odd-even configuration. The following table lists the Exit Router port assignments when used in M3 Zone Core configurations.

Table 42: Exit Router Cabling – M3 Zone Core Configuration

Exit Router	Port	Device/Function
Exit Router 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access
Exit Router 2	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access

3.7.2.2 Cabling the Exit Router to the CWR Relay Panel

Connect the relay panel to the exit router with the T1/E1 connectors through the 12-port relay cables. For more information, see the *Cooperative WAN Routing* manual.

3.7.2.3 Cabling the Exit Router to the Core Backhaul Switch

If Ethernet site links are implemented to one or more sites, the third Ethernet port on each of the two exit routers is connected to the two core backhaul switches. They provide the link through the Ethernet backbone to the other zones.

3.7.3 Exit Router – Maintenance and Troubleshooting

Generic maintenance and troubleshooting procedures apply. For maintenance and troubleshooting information, see S6000 Introduction, Installation, and Configuration on page 27.

3.7.3.1 Exit Router Failures

Exit routers are installed in pairs. Because of this redundancy, failure of one exit router is transparent to the user.

- If an exit router fails, the redundant router takes over.
- If both routers fail, the network of the connected zone is isolated and InterZone Local Area Network (LAN) traffic to other zones is lost.

Exit router failures are reported in the fault management application and additional router details are available through the UNC. When a failure is suspected, perform the appropriate field replaceable entity (FRE) replacement procedures.

3.8 GPRS Gateway Support Node (GGSN) Router (M and L Zone Cores)

The GPRS Gateway Support Node (GGSN) router handles network traffic between the Motorola Solutions radio network infrastructure and external networks to support data services.

NOTICE: The GGM 8000 can be used as a replacement for the S6000 GGSN (GPRS Gateway Support Node) employing Ethernet site links. See the *GGM 8000 System Gateway* manual for details.

3.8.1 GGSN Router – Functional Description

Implementation of GPRS Gateway Support Node (GGSN) functionality on Motorola Network Router (MNR) S6000 routers enables data capability. The GGSN tunnels packet data through private networks to mobile subscribers, thereby allowing the mobile subscribers to access the Customer Enterprise Networks (CENs) to which they belong.

A mobile subscriber typically consists of a mobile computer attached to a mobile radio through a serial or USB connection. The mobile radio performs all mobility tasks on behalf of the mobile computer.

A GGSN router serves as a network interface between the Motorola Solutions radio network and the CEN. One side of the router connects to the Motorola Solutions Radio Network Infrastructure (RNI). The other side attaches to a peripheral network to interface with the border routers of the CEN. Redundant GGSN routers are used to support HA (High Availability) Data and DSR Data.

The GGSN provides General Packet Radio Service (GPRS) network access to external hosts to communicate with mobile subscribers. The GGSN acts as a fixed relay point between the external hosts and the mobile subscribers.

A GGSN router is designed to handle IP routing services for end-to-end data messaging for Trunking and/or Conventional ASTRO® 25 systems that support High Performance Data (HPD) and IV&D. The functions of a router include the following:

- Network address translation for static and dynamic IP addressing and IP fragmentation
- Secure IP tunneling
- Internet Control Message Protocol (ICMP) error reporting for troubleshooting activities

Each HPD and IV&D system has one GGSN router or more per system. The GGSN router provides the following HPD and IV&D support functions:

- Isolates your organization's wireline and wireless network traffic from the Motorola Solutions RF network
- Facilitates the use of your organization's Dynamic Host Configuration Protocol (DHCP) servers as well as the IP plan
- Isolates your agencies

A GGSN router provides a logical interface to the Packet Data Router (PDR) module in the Packet Data Gateway (PDG). It maintains routing information for all attached packet data users. Routing information is used to tunnel through GPRS Tunneling Protocol (GTP) user datagrams to the current point of attachment of each Mobile Subscriber Unit (MSU). The attachment is the home PDR to your hosts through IP-IP tunnels.

3.8.1.1 Manual GGSN Switchover

In the event of failure, redundant GGSN routers provide an automatic switchover, but the user also has the option to initiate a switchover manually. A manual GGSN switchover is executed from the Unified

Network Configurator (UNC) by performing a reboot of the primary GGSN router. The reboot causes the redundant GGSN to take over.

See the *Unified Network Configurator* manual for the router reboot procedure.

3.8.1.2
GGSN – Network Connections

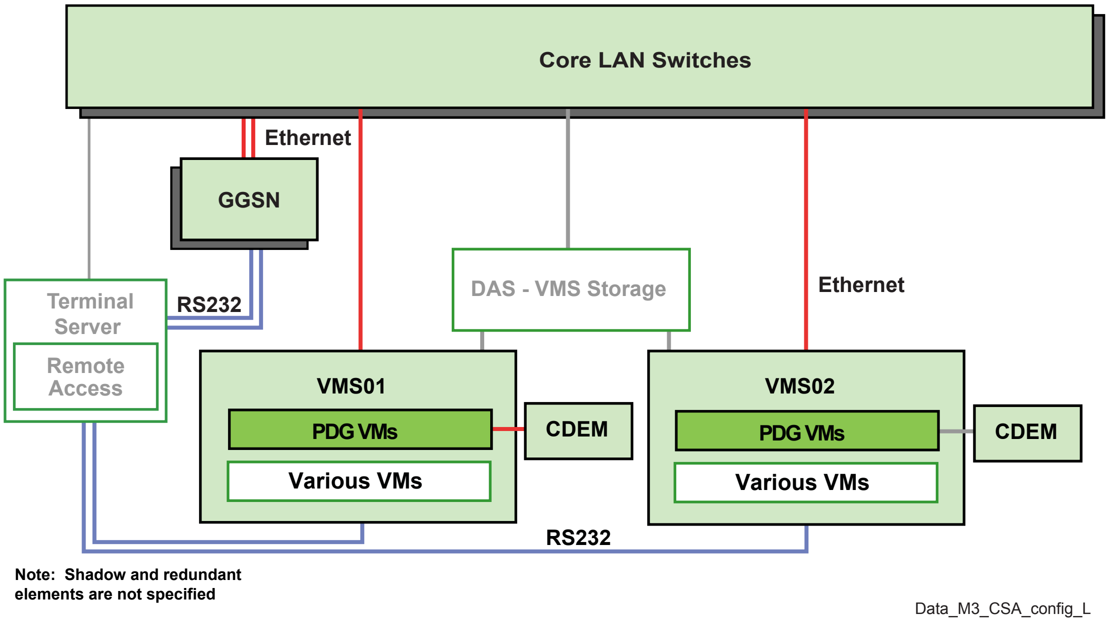
The GGSN router has two 100Base-T connections to the LAN switch to tunnel traffic between the HPD or Trunking and/or Conventional IV&D Packet Data Gateway (PDG) and a border router. The border router routes the traffic for the CEN. It also has a serial connection to the terminal server, enabling router administration.

The following diagram shows the GGSN router connections at the master site. See Master Site Routers – Network Connections on page 110 for a master site diagram showing the GGSN router.

NOTICE: This diagram shows the connection of the IV&D PDG to the GGSN through the LAN switch. The placement of the PDG is the same regardless of whether it is an IV&D PDG, an HPD PDG, or a Conv PDG.

See the *Dynamic System Resilience Feature Guide* manual for additional configurations.

Figure 34: GGSN Router Connections



Note: Shadow and redundant elements are not specified

Data_M3_CSA_config_L

3.8.1.3
Charging Gateway Interface

The Charging Gateway provides a mechanism for GGSN to collect usage statistics for data calls and forward them to your organization's billing interface, which exists outside the ASTRO® 25 system Radio Network Infrastructure (RNI) in the Customer Enterprise Network (CEN). This is achieved by switching on the charging function in the GGSN. The GGSN generates Call Detail Records (CDR), which it then forwards to the Charging Gateway Function (CGF) located in the DMZ, which in turn forwards the data to an external billing system in the CEN for further processing. The external billing system is considered to be part of your system, and is not provided as part of Motorola Solutions Radio Network Infrastructure (RNI).

3.8.1.4 GGSN Functions

The GGSN performs the following specific functions:

- Forwards outbound traffic to the appropriate home HPD or IV&D PDRs
- Sends inbound traffic through Virtual Private Network (VPN) tunnels to the appropriate CEN
- Originates/terminates the GTP tunnels to the Conventional HPD or IV&D PDRs, and the IP-IP tunnels to the CENs
- Sends dynamic updates to the Dynamic Domain Name Service (DDNS) server on the CEN for MSUs after context activation, if configured
- Queries the RADIUS or DHCP server on the CEN for authentication or dynamic addressing, if configured
- Provides local dynamic addressing for MSUs, if configured
- Collects usage statistics for data calls through the Charging Gateway and forwards them to your organization's billing interface

The GGSN originates IP-IP tunneling to the CENs. The IP-IP tunnels provide secure data delivery traffic to the CENs over the peripheral network. The IP-IP tunneling also provides IP isolation between the system and the CENs to prevent IP address conflicts.

The GGSN is configured with an Access Point Number (APN) for each CEN. The APN is mapped to the physical or virtual ports assigned for each of the CEN border routers. Each MSU is assigned to a particular CEN or APN through the Provisioning Manager application. When the GGSN receives inbound traffic, it forwards the traffic to the appropriate CEN, depending on the APN.

The GGSN is provisioned to interact with RADIUS, DHCP, and DDNS servers on each CEN. The GGSN queries the RADIUS server on the CEN with authentication credentials received from the context-activating MSU. It permits mobile users to authenticate with the CEN during the context activation process.

Depending on the MSU and system configuration, the GGSN also queries the DHCP server on the CEN to receive dynamic addresses for context-activating MSUs. When a RADIUS server is used at the CEN, it operates as both an authentication server and a DHCP server. Otherwise, the GGSN is configured with its own pool of IP addresses to locally provide dynamic addresses to context-activating MSUs.

The GGSN is configured to supply dynamic updates to a DDNS on the CEN. These dynamic updates provide Fully Qualified Domain Name (FQDN) bindings for each context-activating MSU. This FQDN consists of a host name plus the domain name for the MSU (such as: c620100000e0df659f.hpd.cen20). It allows CEN hosts to access the MSUs by using the FQDN associated with an MSU instead of its IP address.

3.8.1.5 GGSN Functional Requirements

Motorola Solutions GGSN functionality requires the following:

- S6000 router with an IP path to each HPD, IV&D, or Conv PDG and your organization's border router
- EOS software certified for this system release, that supports GGSN (GS or GW package)
- EOS software configuration for GGSN service:
  - Virtual ports configured to connect to the CEN domain
  - APN profiles created to configure IP address allocation
  - GGSN control enabled

The PDG consists of the PDR and the Radio Network Gateway (RNG). It performs the functions of a Serving General Packet Radio Service Support Node (SGSN) and mobility. The GGSN software configuration is contained in the XGSN.cfg configuration file.

NOTICE: The XGSN.cfg file is also known as the xgsn.cfg file.

3.8.2

GGSN Router – Installation and Configuration

Prerequisites: Ensure that you have the required cabling and connectors.

Process:

1. Install the GGSN router in a rack. See S6000 Introduction, Installation, and Configuration on page 27.
2. Connect the GGSN router to the power source. See S6000 Introduction, Installation, and Configuration on page 27.
3. If necessary, ground the GGSN router. See S6000 Introduction, Installation, and Configuration on page 27.
4. Connect the GGSN router to the master site LAN switch. See GGSN Router – Site-Specific Cabling on page 129.
5. Configure the GGSN router. See S6000 Introduction, Installation, and Configuration on page 27.

3.8.2.1

GGSN Router – Site-Specific Cabling

Connect GGSN routers to the master site LAN switches in an odd-even configuration. The following table lists the GGSN Router port assignments when used in M zone core configurations.

Table 43: GGSN Router Cabling – M1 and M2 Zone Core Configurations

GGSN Router	Port	Device/Function
GGSN Router 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 1
	RS-232	Terminal Server or Local Serial Access

Table 44: GGSN Router Cabling – M3 Zone Core Configuration

GGSN Router	Port	Device/Function
GGSN Router 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	RS-232	Terminal Server or Local Serial Access
GGSN Router 2	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	RS-232	Terminal Server or Local Serial Access

3.8.2.2

Configuring GGSN Charging Parameters

For comprehensive information on configuring charging parameters, see the “GGSN Router Management” section in the *Unified Network Configurator* manual.

3.8.2.3

GGSN Configuration (xgsn.cfg) File Management

When the GGSN gateway is enabled, the gateway supports a GGSN configuration (`xgsn.cfg`) file in addition to the `boot.cfg` and `acl.cfg` configuration files. The `xgsn.cfg` file includes GGSN, virtual port, and APN configurations. The TNCT file, supplied by Motorola Solutions, creates the `xgsn.cfg` file and contains the GGSN configuration parameters and the APN configuration commands for the APNs. When there is no `boot.cfg` file in the GGSN gateway, the `xgsn.cfg` file does not execute. The `boot.cfg` file executes first, then the `xgsn.cfg` file. The Unified Network Configurator (UNC) VoyenceControl application uses templates to manage the `xgsn.cfg` file.

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

The `xgsn.cfg` file provides GGSN configuration manageability. When booting a router running a software package that supports the GGSN, the `xgsn.cfg` file is used for GGSN configuration commands. It includes GGSN configuration commands in the `boot.cfg` file. A `boot.cfg` file with GGSN configuration commands causes logging errors when used on a router running a software package that does not support the GGSN.

See the “GGSN Router Management” section in the *Unified Network Configurator* manual.

3.8.2.4

Allocating IP Addresses for Mobile Subscribers

IP addresses for mobile subscribers are allocated in one of the following ways:

- **Static subscriber IP address allocation** – The IP assigner is set to the local DHCP, but no address pools are configured. All requesting subscribers are assigned statically; the User Configuration Server application (UCS) assigns proposed IP addresses before the Packet Data Protocol (PDP) context create reaches the GGSN.
- **Dynamic subscriber IP address allocation through a local server** – The IP Assigner is set to the local DHCP with address pools configured. The Border router assigns the IP addresses from this pool to a requesting mobile subscriber during PDP context establishment. The GGSN router allocates one or more sets of IP addresses dynamically from a block of available addresses configured per APN from the CEN’s address space. The GGSN requests an IP address from the Border router configured IP pool on behalf of the mobile subscribers. The IP addresses can be assigned dynamically from a configured pool. They can also be reserved and specifically matched to the International Mobile Subscriber Identity (IMSI) numbers.
- **Dynamic subscriber IP address allocation through a DHCP server** – The IP Assigner is set to Remote DHCP. A DHCP server, located within the address space of the CEN, assigns the subscriber addresses dynamically. The GGSN requests IP addresses from the DHCP server on behalf of mobile subscribers.
- **Dynamic subscriber IP address allocation through a RADIUS server** – A RADIUS server, located within the address space of the CEN, assigns the subscriber addresses dynamically. Authentication is performed by the same RADIUS server. Authentication is required when IP addresses are allocated through a RADIUS server. The GGSN requests IP addresses and authentication from the RADIUS server on behalf of mobile subscribers.

3.8.2.5 Adding New APNs

The Unified Network Configurator (UNC) supports the GGSN DDNS feature. It allows for the retrieval of the IP address of a specific mobile subscriber from the DNS server on the CEN.

In the data flow process, the GGSN does the following:

- Receives a PDP context create message from the PDR during the context activation
- Opens the context when the optional RADIUS authentication process passes
- Stores the IP address of the mobile subscriber in the following ways:
  - Proposes in the context create message
  - Allocates from the Border router configured IP address pool
  - Allocates from the external DHCP service
  - Allocates from the external RADIUS services
- Sends out UDP-based dynamic DNS update messages to the DNS server located in the CEN
- Starts a retransmission timer after sending out a dynamic DNS update request

When the dynamic DNS response is not received, the GGSN retransmits the update request three times at five second intervals. It does not deactivate the PDP context. Dynamic DNS update messages sent by the GGSN include:

- A resource record that specifies the IP address of the mobile subscriber for DNS forward lookup.
- A PTR resource record that specifies the FQDN of the mobile subscriber for DNS reverse lookup.

The information about the mobile subscriber is registered by the Fully Qualified Domain Name (FQDN) and the assigned mobile IP address. The formatting for the FQDN is **MSISDN.DDName**.

NOTICE: When the GGSN receives a dynamic DNS update response in the middle of a retransmission, it stops the retransmission and frees up the retransmission timer.

To configure a GGSN router for dynamic DNS functionality, specify the IP address of the DNS server and the DDNS server name when configuring the APN on the GGSN. Use the templates in the UNC to create, view, and edit the APN configuration parameters for the GGSN router.

See “Creating an APN” and “Access Point Name Management” sections in the *Unified Network Configurator* manual.

3.8.2.6 Configuring Overload Protection Management (OPM)

The MNR router software applications are designed for memory usage and CPU utilization within the acceptable margins, based on the required messages-per-hour rate.

For example: The GGSN application performs adequately by limiting the number of simultaneous contexts open at all times. When a packet or a data storm occurs, the packet rate increases above the stated required maximum. In such cases, limited data loss occurs in arbitrary places in the data pipeline of the router.

The purpose of the Overload Protection Management (OPM) feature is to monitor the following parameters and to inform registered applications (OPM clients) when any of the parameters meet or exceed the configured threshold.

- CPU utilizations
- Memory utilization
- Queue drop

The registered applications limit their activity during overload conditions, thereby preventing potential data loss.

NOTICE: In the initial release of the OPM, queue drops are accumulated for Ethernet ports only.

The initial release of the OPM supports the following two clients: GGSN and SNMP.

The OPM thresholds for each of the monitored parameters can be set to high, medium, or low. Each threshold level (high, medium, or low) is associated with internally configured high-water and low-water marks. OPM clients are called when either of the following events occurs:

- Overload – The parameter meets or exceeds the high-water mark associated with the specified threshold level (high, medium, or low).
- Normal – The parameter falls below the low-water mark associated with the specified threshold level (high, medium, or low).

NOTICE: The EOS implementation of overload protection management incorporates a 30-second Holddown timer, which prevents the router from entering or leaving Overload within that time period. For example, if a router enters Overload state at 3:30:15, the Holddown timer starts and the router cannot exit Overload state until the 30-second Holddown period expires (in this example, at 3:30:45).

The registered GGSN application takes the following appropriate actions when it discovers an overload:

- Reads the number of active PDP contexts (GTP tunnels)
- Freezes the number of active contexts at that value
- Rejects any new context creates until one of the following scenarios occurs:
  - An existing context is dropped when one new context is created for every existing context create.

    NOTICE: The maximum configurations of contexts created is 65,535. When no limit is configured, the default limit is 20,000.
  - A received normal event indicates that the monitored parameter falls below the low-water mark associated with the configured threshold.
- Sends a trap when it receives an Overload or a Normal event

3.8.2.6.1 Configuring a Router for Overload Protection

To activate the overload protection using Unified Network Configurator (UNC), see “Managing GGSN Router Statistics” section in the *Unified Network Configurator* manual.

3.8.2.6.2 Retrieving Overload Protection Statistics

You can retrieve the following overload protection statistics:

- CPU Utilization – The current value for CPU utilization.
- Memory Usage – The current value for memory usage.
- Queue Drops – The current value for queue drops.
- The number of times the router has gone into Overload state.
- A log of the last five times the router went into Overload state, including the following information:
  - Start Time – The time at which the router went into Overload state.
  - End Time – The time at which the router exited the Overload state.

- Duration – The amount of time the router was in the Overload state.
- Cause In – The reason why the router went into the Overload state (CPU utilization, memory usage, or queue drops).
- Cause Out – The reason why the router exited the Overload state (CPU utilization, memory usage, or queue drops).

For information how to manage the overload protection statistics in the Unified Network Configurator (UNC), see the "Managing GGSN Router Statistics" section in the *Unified Network Configurator* manual.

3.8.3 GGSN Router – Operation

This topic provides user operation procedures for working with Access Point Number (APN) information and viewing statistics for the GGSN.

3.8.3.1 Viewing and Editing Existing APNs

To view and edit existing GGSN parameters, see the "GGSN Router Configuration File Management" section in the *Unified Network Configurator* manual.

3.8.3.2 Viewing Statistics

You can gather and display the following GGSN GTP statistics:

- GTP Peer IP Address – The IP address of the GTP tunnel peer.
- State – The operational status of the GTP tunnel (UP or DOWN).
- Number of PDP Contexts – The currently configured maximum number of PDP contexts supported on the GGSN router.
- Received Control Packets – The total number of control packets received from all IV&D, HPD, or Conv PDGs (Packet Data Gateways).
- Sent Control Packets – The total number of control packets sent to any CEN.
- Received Data Packets – The total number of data packets received from all IV&D, HPD, or Conv PDGs.
- Received Data Bytes – The total number of data bytes received from all IV&D, HPD, or Conv PDGs.
- Sent Data Packets – The total number of data packets sent to any CEN.
- Sent Data Bytes – The total number of data bytes sent to any CEN.
- Mobile IP Services – The total number of mobile node registrations sent from all Conv PDGs and received by any CEN.

3.8.3.2.1 APN Statistics

You can gather and display statistics for APN. To view APN statistics, see "Showing APN and RADIUS Statistics" in the *Unified Network Configurator* manual.

CEN Statistics

Statistics for User Data

Sent Packets
The total number of packets sent to CEN through this APN

Rcvd Packets
The total number of packets received from CEN through this APN

Sent Bytes
The total number of bytes sent to CEN through this APN

Rcvd Bytes
The total number of bytes received from CEN through this APN

SHow stat–MOBileIP
The total number of mobile node registrations sent from all Conv PDGs and received by any CEN.

Statistics for DDNS

Sent DDNS Update Req
The number of DDNS update request messages sent to the DNS server in CEN

Rcvd DDNS Update Rsp
The number of DDNS update response messages received from the DNS server in CEN

Rcvd DDNS Update Err
The number of received DDNS update responses, which indicate an error in the DNS update

ReXmt DDNS Update Req
The number of retransmissions for DDNS update request messages

DDNS Update Timeout
The number of DDNS update request messages that were retransmitted and eventually timed out

Statistics for DHCP

Sent DHCP Discover
The number of DHCP discover messages sent to the DHCP server in CEN

Rcvd DHCP Offer
The number of DHCP offer messages received from the DHCP server in CEN.

Sent DHCP Req
The number of DHCP request messages sent to the DHCP server in CEN

Rcvd DHCP Ack
The number of DHCP Ack messages received from the DHCP server in CEN

Sent DHCP Release
The number of DHCP release messages sent to the DHCP server in CEN

Rcvd DHCP Rsp Err
The number of received DHCP response messages indicating an error

DHCP Discover Timeout
The number of DHCP discover messages that were retransmitted and eventually timed out

DHCP Req Timeout
The number of DHCP request messages that were retransmitted and eventually timed out

DHCP Switchover
The number of switchovers from primary to secondary or secondary to primary DHCP servers

DHCP
The IP address of the current external DHCP server

RADIUS Auth.
The IP address of the current RADIUS authentication server

RADIUS Acct.
The IP address of the current RADIUS accounting server

Authentication Statistics

Switchovers

The number of switchovers from primary to secondary or secondary to primary RADIUS authentication servers

Accepts

The number of authentication accept messages received from the RADIUS server

Rejects

The number of authentication reject messages received from the RADIUS server

Timeout

The number of context creation failures caused by authentication timeout

Retries

The number of authentication message retransmissions

Max RoundTrip

The maximum response time from the first authentication request message to the time when the response is received. It may include retransmissions.

Accounting Statistics

Switchovers

The number of switchovers from primary to secondary or secondary to primary RADIUS accounting servers

Success

The number of accounting start response messages received from the RADIUS server

Failure

The number of failures on the accounting start response messages received from the RADIUS server

Timeout

The number of timeouts on accounting start response messages

Duplicated IP

The number of RADIUS-allocated IP addresses, which are duplicated in the GGSN router

Max RoundTrip

The maximum response time from the first accounting start response message to the time when the start response is received. It may include retransmissions.

High Availability Statistics

Real Time Contexts Sent to Standby

The number of contexts that the Master GGSN sends to the StandBy GGSN

Number of Times Peer Came Up

A counter that increments after port 1 of the peer GGSN comes back **UP** after being disabled

Number of Times Peer Went Down

A counter that increments after port 1 of the peer GGSN goes **DOWN**

Number of HA Switchovers

This counter increments every time the HA vrrp Mastership gets switched from the Master GGSN to StandBy GGSN and reverse

3.8.4 GGSN Router – Maintenance and Troubleshooting

This topic provides fault management and troubleshooting information relating to the GGSN routers.

3.8.4.1 General Troubleshooting for the GGSN

If there is a failure on the GPRS Gateway Support Node (GGSN) router, the system loses the ability to provide data messaging from your data network to mobile data devices in your system and all IP services are dropped. When a GGSN router fails, the Packet Data Router (which this router interfaces to) sends “link down” status information to Unified Event Manger (UEM) server in that zone. The GGSN Link object in the UEM displays the reported status of the logical link between the PDR and the GGSN router.

If Dynamic System Resilience (DSR) is implemented on your system, the MNR routers support multiple IPIP tunnels per APN for redundancy. This feature supports the GGSN Dynamic System Resilience configuration. APN to multiple IPIP binding allows the system to support DSR to multiple Customer Enterprise Networks (CENs). When the link for one of the tunnels fails, the router switches over to the other IPIP tunnel, thereby preserving connectivity between the GGSN and the CEN.

NOTICE: Multiple IPIP tunnels are supported only for redundancy, and only one tunnel is active at a time.

To bind an APN to multiple IPIP tunnels, a bidirectional forwarding detection (BFD) gateway IP address (the IP address of the border router) and a priority value for each tunnel is specified when the APN is configured in the UNC. BFD maintains the link status for each tunnel and informs the GGSN software when a link comes up or goes down. When the GGSN receives a status change notification, it transparently uses the active IPIP tunnel with the highest priority value to connect to the CEN. If that tunnel fails, the GGSN switches over to the other IPIP tunnel until the higher priority link is re-established.

The GGSN sends an alarm to the UEM both when the GGSN connection to the CEN has been established and when the GGSN connection to the CEN goes down.

The data port (V1) on the GGSN has a static IP address and does not send any SNMP traps to the UEM.

For more information on the operation of the UEM, a list of devices managed by the UEM, and alarms managed by the UEM, see the *Unified Event Manager* manual.

If High Availability (HA) Data is configured in your system, GGSNs are deployed as a redundant pair. If the active GGSN experiences a failure which makes it unable to provide data service, the redundant GGSN becomes active. Data service is restored within 90 seconds of the failure. In this configuration, the MNR routers support multiple paths (two for HA Data, four for HA Data with DSR) to the Customer Enterprise Networks (CENs). When the active path to the CEN fails, the routers switch over to the next highest priority path. For more information about the HA Data feature and for a failure and recovery scenario of GGSN HA Data subsystem routers, see the *Trunked Data Services Feature Guide* manual.

3.8.4.2 Understanding Dynamic Configuration through the UNC

The Unified Network Configurator (UNC) uses VoyenceControl to configure and monitor the status of the GGSN service on S6000 routers. Using the GGSN management function, the GGSN configurations are viewed, created, and modified by using templates.

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

The templates include:

- Managing the GGSN router configuration files. The XGSN.cfg file contains the GGSN configuration parameters.
- Managing the Access Point Number (APN) parameters, which are configuration commands for the APNs configured on the device.

The step-by-step procedures are located in the “UNC Operation” chapter of the *Unified Network Configurator* manual.

Chapter 4

ASTRO 25 Repeater Site

This chapter provides information on the S2500 router in an ASTRO® 25 system Repeater Site.

4.1 Repeater Site Router – Functional Description

The site router at the remote site supports traffic between the master site and the remote site Local Area Network (LAN). The site router directs all voice, control, and network management traffic between the master site and the remote site. An optional redundant site router can be installed. At a repeater site, the Motorola Network Router (MNR) S2500 router is used to provide connectivity from the LAN to the master site zone controller, zone manager, network management servers, and MOSCAD Network Fault Management (NFM) equipment.

The site can be set up to benefit from the zone core redundancy afforded by Dynamic System Resilience (DSR), or designed to connect to one zone core only as in systems without DSR. For detailed information on the DSR configuration, see the *Dynamic System Resilience Feature Guide* manual in this documentation set.

The remote site router links the ASTRO® 25 repeater sites to the master site. It provides a network interface for the flow of voice, control, data, and network management traffic over these links.

The site router also serves as the Ethernet transport interface to the Ethernet backbone on systems that implement the Flexible Ethernet Links feature. If the Flexible Ethernet Links feature is implemented on the system, the site router is equipped with an Ethernet module that connects to the Ethernet backbone. See the *Flexible Site and InterZone Links* manual for details.

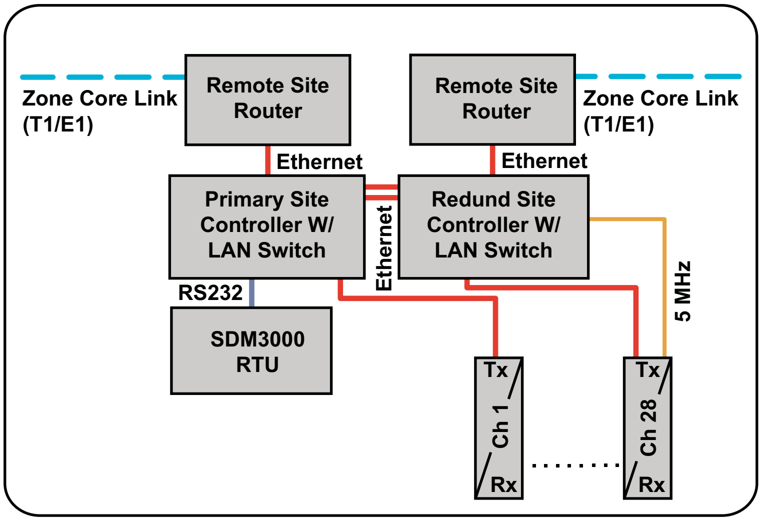
Components

The site router for the repeater site may have different components and connections, depending on whether a circuit-based Conventional channel is supported at the site.

- **If a circuit-based Conventional channel is supported**: One of the site routers has an Ethernet connection to the site LAN and a V.35 serial connection to the High-Speed Unit (HSU) card on the channel bank. In this configuration, the site router delivers traffic from the site LAN over frame relay to the channel bank. The channel bank multiplexes the traffic from the site LAN with circuit-based Conventional channel traffic and delivers the traffic to the master site over a channelized T1/E1 link.
- **If a circuit-based Conventional channel is not supported or if a redundant site router is installed**: The site router has one Ethernet connection to support traffic to the site LAN, and one T1/E1 connection to the T1/E1 link to the master site. The site routers at the repeater site handle all voice, control, and network management traffic going in and out from the site, except circuit-based Conventional channel traffic.

Typically, routers at the repeater site interface with the components shown in the figure below.

Figure 35: ASTRO 25 Repeater Site – Components



S_ASTRO_25_Repeater_Site_C

NOTICE:

- The diagram shows T1/E1 links to the master site and to the remote site. For connection diagrams showing Flexible Ethernet Links, refer to the *Flexible Site and InterZone Links* manual.
- If the Dynamic System Resilience is implemented on your system, refer to the *Dynamic System Resilience Feature Guide* manual for details on connections and diagrams relating to the site router.
- The remote site router in the ASTRO® 25 repeater site can support conventional channel resources. For details, see the *Conventional Operations* manual.
- Hybrid site links for redundant site links can also be implemented. See Hybrid Site Link Overview on page 121.

Repeater Site Routers Functions

Media conversion

The router converts the 100 MB Ethernet LAN packets to IP packets encapsulated in Frame Relay on a serial WAN interface, or to tunneled IP packets on an Ethernet flexible site link.

Traffic prioritizing

The router applies the correct prioritization masking to the packets leaving the site.

Fragmentation

The router fragments large IP packets per standards.

Dynamic Host Configuration Protocol (DHCP) service

The router supports DHCP. This service allows the technician with a properly configured service laptop to connect to the LAN at the site.

Redundancy

There can be two routers at the remote site to provide redundancy. The redundant remote site router (optional) along with the redundant links to the redundant router provides protection from single router failure or site link failure.

4.2 Repeater Site Router – Installation and Configuration

Follow this process to install the repeater site router.

Prerequisites: Ensure that you have the required cabling and connectors.

When and where to use: Follow these steps to install and configure the router.

Process:

1. Install the repeater site router in a rack. See S2500 Introduction, Installation, and Configuration on page 66.
2. Connect the repeater site router to a power source. See S2500 Introduction, Installation, and Configuration on page 66.
3. If necessary, ground the repeater site router. See S2500 Introduction, Installation, and Configuration on page 66.
4. Connect the repeater site equipment to the repeater site router. See the following sections related to repeater site router cabling.
5. Configure the repeater site router. See S2500 Introduction, Installation, and Configuration on page 66.

4.2.1 Cabling – Site Router

The site router cabling depends on whether:

- Circuit-based Conventional channels are supported at the ASTRO® 25 repeater site. Depending on the system design, the site may either be configured with a TeNSr channel bank (sites with circuit-based Conventional channels), or the site router may be connected directly with the Wide Area Network (WAN) (sites without Conventional channels).
- Conventional channel resources are supported at the ASTRO® 25 repeater site.
- The Dynamic System Resilience (DSR) configuration is implemented on your system.

4.2.2 Repeater Site Router Cabling – with Dynamic System Resilience

Normally, the connections are made from the site router(s) to one zone core only. If the site is set up to benefit from the zone core redundancy afforded by Dynamic System Resilience (DSR), the connections are made to both primary and backup zone cores.

NOTICE: Contact your system administrator or see your customized system configuration plan for site router port connections in a DSR scenario. For detailed information on the DSR configuration, see the *Dynamic System Resilience Feature Guide* manual.

4.2.3 Repeater Site Router Cabling – without Circuit-Based Conventional Channel

The following table lists generic connections between the site router and other devices at the repeater site without circuit-based Conventional channel equipment.

Table 45: Repeater Site Router Cabling Without Circuit-Based Conventional Channel Cable Connections

From Router		To Destination Device		
Port	Connector type	Port	Connector type	Description
LAN 1	RJ-45	Port 1, Ethernet LAN Switch	RJ-45	Communications connection between the S2500 repeater site router and the Ethernet LAN switch.
I/O Module A (T1/E1)	RJ-45	T1 or E1 from carrier	RJ-45	This T1/E1 link connects the repeater site through the router to the master site, if the repeater site does not have a circuit-based Conventional channel. A T1/E1 I/O module (ST2512) must be installed in the S2500 to make this connection.

NOTICE: See the customized cabling and configuration information provided by Motorola Solutions for port connections specific to your system.

4.2.4 Repeater Site Router Cabling – with Circuit-Based Conventional Channel

The following table lists generic connections between the site router and other devices at the repeater site with circuit-based Conventional channel equipment.

Table 46: Repeater Site Router Cabling with Circuit-Based Conventional Channel

From Router		To Destination Device		
Port	Connector type	Port	Connector type	Description
LAN 1	RJ-45	Port 1, Ethernet LAN Switch	RJ-45	Communications connection between the S2500 repeater site router and the Ethernet LAN switch.
FlexWAN Serial	V.35	TeNSr channel bank	RJ-45	Circuit-based Conventional channel link. This link lets the router communicate with the analog circuit-based Conventional channel transceiver through the channel bank. A FlexWAN I/O module

From Router		To Destination Device		
Port	Connector type	Port	Connector type	Description
				(ST2511) must be installed in the S2500 to make this connection.

NOTICE: See the customized cabling and configuration information provided by Motorola Solutions for port connections specific to your system.
The S2500 Remote Site Router with ST2511 FlexWAN module can be replaced with a Site Gateway (FlexWAN) device. The S2500 Remote Site Router with the ST2511 FlexWAN (V.35 serial interface) module supporting ASTRO® 25 Repeater Sites or Circuit Simulcast Remote Sites with circuit-based Conventional channels is replaced with the Site Gateway (FlexWAN) device. See “Replacing Daughterboards on the GGM 8000” procedure in the *System Gateways – GGM 8000* manual.

4.2.5

Repeater Site Router Cabling for Flexible Ethernet Links – without Circuit-Based Conventional Channel

The following table lists the connections between the site router and other devices at a repeater site without a circuit-based Conventional channel that implements Flexible Ethernet links.

Table 47: Repeater Site Router for Flexible Ethernet Links Without Circuit-Based Conventional Channel Cable Connections

From Router		To Destination Device		
Port	Connector type	Port	Connector type	Description
LAN 1	RJ-45	Port 1, Ethernet LAN Switch	RJ-45	Communications connection between the S2500 repeater site router and the Ethernet LAN switch.
Ethernet module (Port 2)	RJ-45	Ethernet backbone	RJ-45	This link exists between the router and the Ethernet backbone. Ethernet module (ST2510) must be installed in slot A of the S2500 router to make this connection for Flexible Ethernet links.

NOTICE: For more details on Flexible Ethernet site links, see the *Flexible Site and InterZone Links* manual.

4.2.6 Repeater Site Router Cabling to Support Analog Conventional or Digital Conventional Resources

The following table lists the connections between the site router and other devices at a repeater site to support ASTRO® 25 Conventional channel resources.

Table 48: Repeater Site Router Cabling to Support Analog Conventional or Digital Conventional Resources

From Device		**To Device**		
Port	**Connector type**	**Port**	**Connector type**	**Description**
LAN 1	RJ-45	Port 1, Ethernet LAN Switch	RJ-45	Communications connection between the S2500 repeater site router and the Ethernet LAN switch.
I/O Module A	V.24 (RJ-45)	Modem or Base Station	RJ45-to-25 "D" adapter or RJ-45	Use these connections when the remote site router is used as a digital CCGW to support ASTRO® 25 Conventional channel resources.
Analog Module	E&M (RJ–1CX)	Base station	N/A	Use these connections when the remote site router is used as an analog conventional channel gateway (CCGW). **IMPORTANT:** The analog interface of CCGW is designed to connect directly to analog stations that are physically located in the same room or building, or through a connection provided by a microwave link. If analog lines are used to connect CCGW to an analog station at another location, a primary surge suppression device must be installed.

For more details, see the *Conventional Operations* manual.

4.3 Repeater Site Router – Maintenance and Troubleshooting

Generic maintenance and troubleshooting procedures apply. For maintenance and troubleshooting information, see S2500 Introduction, Installation, and Configuration on page 66.

Chapter 5

ASTRO 25 HPD Site

This chapter provides information on the S2500 router in an ASTRO® 25 system HPD Site.

5.1 HPD Site Router – Functional Description

The HPD site router is responsible for routing all traffic between the equipment at the HPD remote site and the Cooperative WAN Routing (CWR) system at the master site. The site router can be connected to the master site using either T1, E1, fractional T1 (FT1), or fractional E1 (FE1). The Motorola Network Router (MNR) S2500 is used as the HPD site router.

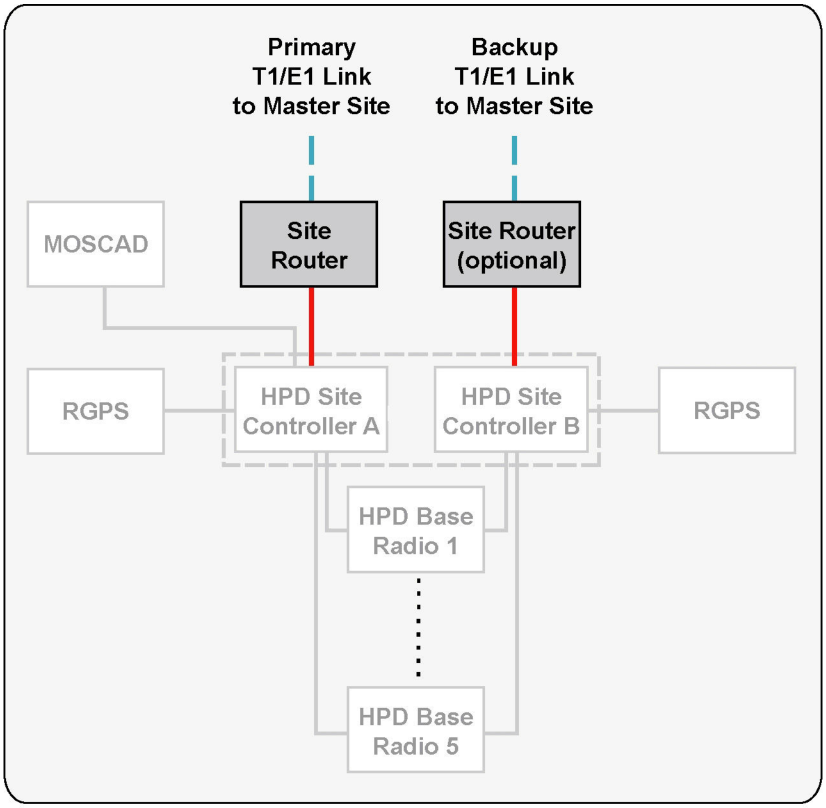
The site can be set up to benefit from the zone core redundancy afforded by Dynamic System Resilience (DSR), or designed to connect to one zone core only as in systems without DSR. For detailed information on the DSR configuration, see the *Dynamic System Resilience Feature Guide* manual in this documentation set.

Ethernet links may also be implemented from the HPD remote site to the master site. The site requires the ST2510 Ethernet module to make this connection. For details, see the *Flexible Site and InterZone Links* manual.

The HPD site router sends all inbound traffic to core routers at the master site, which then forwards the traffic to the next appropriate hop. For all outbound traffic received from the master site, the site router forwards the traffic to the appropriate device on the site LAN.

Depending on the availability requirements for the site, an optional redundant site router can be installed. Redundant site routers operate in an active/standby configuration. Only one path is active at a time. If a failure occurs on the active path (or the primary site controller fails), then the system can revert to the standby path.

Figure 36: HPD Site Routers (Redundant)



S_HPD_RS_comp_routers

The S2500 includes an auto-sensing Ethernet port that connects to the internal LAN switch on the site controller. The ST2512 T1/E1 daughterboard is required to provide the connection to the T1/E1 site link. If conventional channels are being supported at the site, then the following modules are required:

- ST2513 4-wire E&M module is used to support analog conventional channels (Analog CCGW). If a 4-wire module is required, it is installed in the Analog Module slot in the router. The T1/E1 board is installed in the I/O Module A slot.
- ST2514 V.24 module is used when the router supports digital conventional channels (Digital CCGW).

The configuration, backup/restore, and fault management for the router can be performed through the Unified Network Configurator (UNC). The router is pre-configured for the system by Motorola Solutions before it is shipped from the factory.

5.1.1

Remote Site Router

The interfaces provided on the front panel of the HPD remote site router vary, depending on the router function.

An HPD remote site router provides a master site interface only, and features an Ethernet (LAN) port and a T1/E1 port or Ethernet 10 Base-T port. This configuration requires an ST2512 (T1/E1) I/O module or ST2510 Ethernet module. The HPD remote site router can be connected to the master site through a WAN link using either T1 or fractional T1 (FT1) or Ethernet site link.

The HPD remote site router sends all inbound traffic to core routers at the master site, which then forwards the traffic to the next appropriate hop. For all outbound traffic received from the master site, the HPD remote site router forwards the traffic to the appropriate device on the site LAN.

5.1.2 Remote Site Router – Supported Interfaces

The table below provides a descriptive list of interfaces supported by the HPD remote site router.

Table 49: HPD Remote Site Router – Supported Interfaces

Interface	Number of Ports	Description
LAN (Ethernet)	One port (built-in)	LAN ports provide connection to Ethernet LANs using 100Base-TX Ethernet.
T1/E1	One port per module	T1/E1 port that handles master site to remote site interface.
Ethernet	One port per module	Ethernet port that handles master site to remote site interface.
FlexWAN	Serial One port per module	High-speed multifunction serial interfaces that provide connection to industry-standard V.35, RS-232, RS-449, RS-530, or X.21 Data Communications Equipment (DCE) or Data Terminal Equipment (DTE) serial devices. A FlexWAN port provides the interface between an HPD remote site router and the channel bank at a remote site supporting circuit-based Conventional channels.
V.24 module	Two ports per module	V.24 digital interface ports that support an ASTRO® 25 system Conventional Digital CCGW at the site.
Conventional-to-IP (E&M)	Four ports per module	Provides four-wires with E&M relay interfaces to analog conventional base stations. In addition to performing normal IP routing tasks, an S2500 router configured with E&M expansion hardware provides an Analog-to-IP network gateway for analog conventional calls.

5.1.3 Remote Site Router – I/O Modules

The HPD remote site router is a Motorola Solutions S2500 router with one or two I/O modules installed, depending on the router function. It provides a Wide Area Network (WAN) interface that handles all the traffic to and from the zone for the RF site including control, data, and network management traffic. Information sent by the HPD remote site router is handled by the Packet Data Gateway (PDG).

HPD remote site routers support the following network functions:

- Master site interface only: Handles network traffic between the master site and remote site without the need to support circuit-based Conventional channels or remote console sites.
- Circuit-based Conventional channels support: Handles network traffic between the master site and remote site with channel bank support for sites with circuit-based Conventional channels.
- Conventional Channel Gateway (CCGW): Supports conventional channels at the site.

The following table provides a reference list of the HPD remote site routers used in the ASTRO® 25 system.

Table 50: HPD Remote Site Router Functional Description with I/O Modules

Functional Router Description	Slot A (Port 2)	Slot B (Port 3)	Analog Slot Ports 4, 5, 6, 7
Remote Site Router – Master Site Interface Only	ST2512 (T1/ E1) or ST2510 Ethernet	Empty	Empty
Remote Site Router – Circuit-based Conventional channel support	Empty	ST2511 (V.35 Flex-WAN)	Empty
LAN – Only CCGW	Empty	Empty	ST2513A (4W E&M)
Analog CCGW	ST2512 (T1/ E1)	Empty	ST2513A (4W E&M)
Digital CCGW	ST2512 (T1/ E1)	ST2514 V.24 module	Empty or ST2513A (4W E&M). While both the V.24 module (ST2514) and ST2513 may be physically present, only one module is operational.

5.1.4 Remote Site Router – Port Layout

The port layouts for the HPD remote site router are as follows:

- ***<Ethernet Port>*** 100Base-T – 1
- ***<WAN Port>*** (T1 or E1) – 2
- ***<WAN Port>*** (FlexWAN) – 3 (V.35)
- ***<4W E&M>*** (CCGW) – 4 to 7

5.1.5 Remote Site Router – Supported Features

The table below lists the HPD remote site router supported features.

Table 51: HPD Remote Site Router Supported Features

Supported Feature	ASTRO® 25 Multizone HPD Only Router
Single Site Link	Yes
Dual Site Link	Yes
CCGW module	Yes
Circuit-based Conventional channel	Yes

5.1.6 Remote Site Router – Functions

The HPD remote site routers provide the following functions:

- **Media conversion**: The router converts the outgoing Ethernet LAN packets to IP packets encapsulated in Frame Relay on a T1/E1 WAN link.
- **Traffic prioritizing**: The router applies the correct prioritization masking to the packets leaving the site.
- **Fragmentation**: The router fragments large IP packets per standards.
- **Dynamic Host Configuration Protocol (DHCP) service**: This service allows a technician to connect to the LAN at the site using a properly configured PC with the Windows operating system.
- **Redundancy**: There can be two routers at the subsite, which provide redundancy. While one of the routers is operational, the other router is redundant. This optional redundant subsite router along with the redundant links to the redundant router provides protection from single router failure or single WAN link failure.

  NOTICE: Redundancy is an optional configuration.

5.1.7 HPD Remote Site Infrastructure

The network infrastructure at an HPD remote site includes an Ethernet switch built into the site controller and an HPD remote site router. A computer, loaded with the appropriate software, can be connected to a port on the Ethernet switch to conduct programming changes or troubleshooting services.

At the HPD remote site, the S2500 router is used to provide connectivity from the HPD remote site LAN to the master site zone controller, zone manager, Unified Event Manager (UEM), and MOSCAD Network Fault Management (NFM) servers.

5.2 HPD Site Router – Installation and Configuration

Prerequisites: Prepare the required cabling and connectors.

Process:

1. Install the HPD site router in a rack. See S2500 Introduction, Installation, and Configuration on page 66.
2. Connect the HPD site router to a power source. See S2500 Introduction, Installation, and Configuration on page 66.
3. If necessary, ground the HPD site router. See S2500 Introduction, Installation, and Configuration on page 66.
4. Connect the equipment to the HPD site router. See HPD Remote Site Router Cabling on page 153.
5. Configure the HPD site router. See S2500 Introduction, Installation, and Configuration on page 66.

5.2.1

Remote Site Router Connectors

The HPD remote site router features one 100Base-TX Ethernet interface on the base system and one of the following interfaces depending on the router function:

- T1/E1: Used when the HPD remote site router supports master site interface only.
- FlexWAN (V.35): Used when the HPD remote site router supports circuit-based Conventional channels.
- E&M (analog): Used when the HPD remote site router supports analog conventional channels at the site.
- V.24: Used when the HPD remote site router supports digital conventional channels at the site.

5.2.2

Remote Site Router – Cabling the Ethernet Connector

The HPD remote site router features one Ethernet (LAN) connector. Cable the Ethernet (LAN) connector of the HPD remote site router.

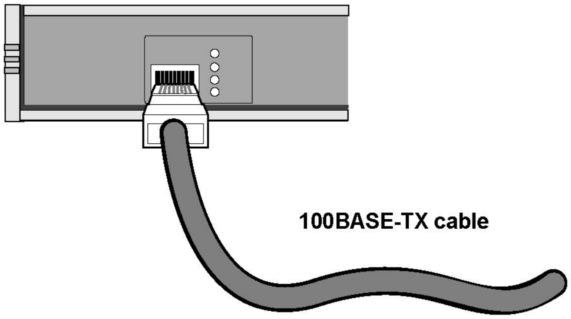
Prerequisites: Prepare:

- 100BASE-TX cable
- Locate the Ethernet (LAN) connector and HPD Site Controller module or junction panel (depending on the type of connection)

Procedure:

1. Connect one end of a 100BASE-TX cable to the HPD remote site router. Connect one end of a 100BASE-TX cable to the HPD remote site router, as shown in figure below.

   Figure 37: Cabling the Ethernet Connector

   S2500_ethernet_connector_cabling

   NOTICE: To cable the Ethernet port on the base system for a 100BASE-TX connection, use a 100BASE-TX cable.

2. Connect the other end of the cable to the HPD Site Controller module or junction panel. See HPD Remote Site Router Cabling on page 153 for details.

5.2.3

Remote Site Router – Cabling the T1/E1 Connector

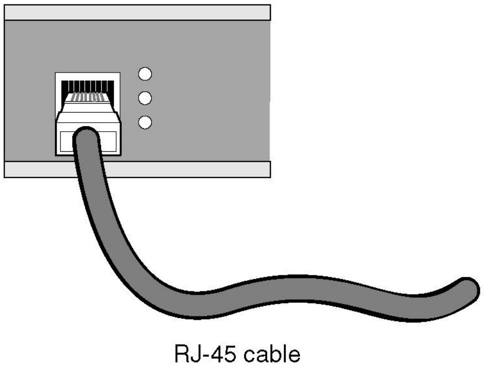
When the HPD remote site router is used for master site interface only, it features one T1/E1 connector. Perform certain steps to cable a T1/E1 connector of the HPD remote site router.

Prerequisites: Prepare an RJ-45 cable.
Locate the primary or backup site link (or CSU/DSU device, depending on the type of connection).

Procedure:

1 Attach one end of an RJ-45 cable to the HPD remote site router, as shown in the following figure.

Figure 38: Cabling a T1/E1 Connector



S2500_WAN_Telco_connector

2 Connect the other end of the RJ-45 cable to the primary or backup site link (or CSU/DSU device). See HPD Remote Site Router Cabling on page 153 for details.

5.2.4

Remote Site Router – Cabling the FlexWAN (V.35) Serial Connector

When the HPD remote site router supports circuit-based Conventional channels, it features one FlexWAN (V.35) connector. This section explains how to cable the FlexWAN serial connector of the HPD remote site router.

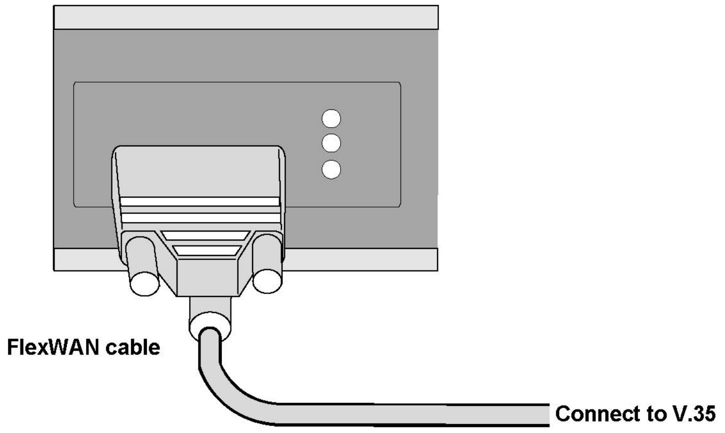
Prerequisites: Prepare:

- Serial (V.35) cable
- Locate the V.35 connector on the channel bank.

Procedure:

1 Connect one end of a serial cable to the 60-pin FlexWAN connector on the HPD remote site router, as shown in the figure below.

Figure 39: Cabling a FlexWAN Serial Connector



S2500_FlexWAN_connector_cabling

2 Connect the other end of the cable to the V.35 connector on the channel bank. See HPD Remote Site Router Cabling on page 153 for details.

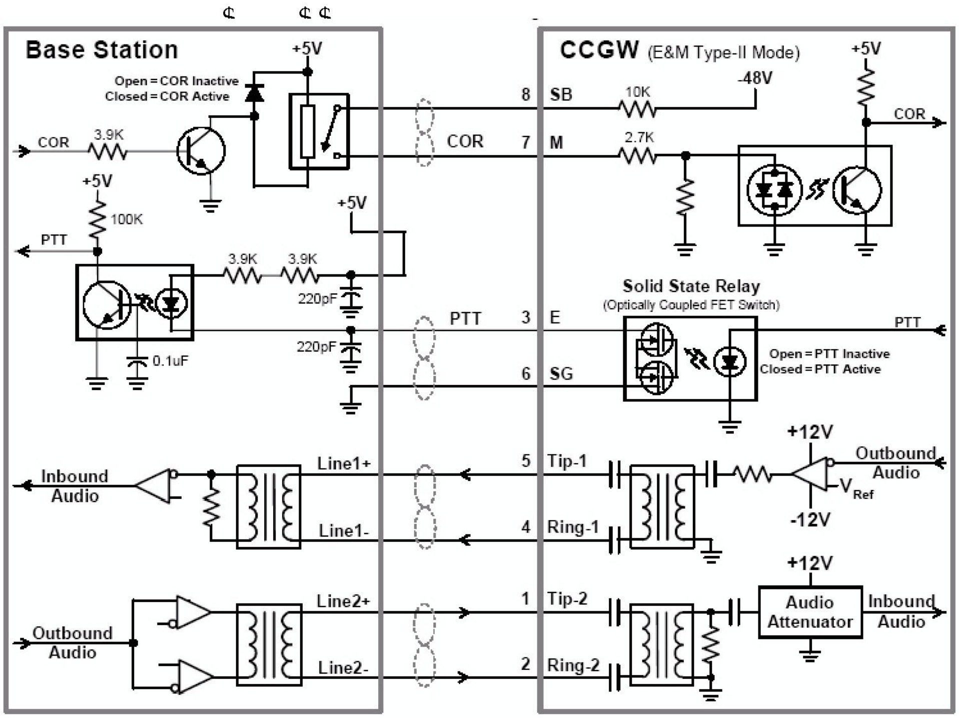
5.2.5

Remote Site Router – E&M (Analog) Connectors

When the HPD remote site router is used to support conventional channels at the site, it features four E&M (analog) connectors to connect the signals on each of the E&M ports with a typical QUANTAR® Base Station.

NOTICE: While QUANTAR® Base Stations do not specifically implement a standard E&M interface, they do include all the components (voltage supplies, relays, and current detectors) necessary to interoperate with the E&M interfaces on the HPD remote site router.

Figure 40: CCGW E&M Port Interconnections with a QUANTAR Base Station



S2500_EM_Port_interconnections_w_QUANTAR

NOTICE: The figure shows a 5-volt supply output on the base station as the voltage source for the current detector on the base station. However, the HPD remote site router safely accepts any voltage source between +/- 60 VDC, if the voltage output of the source does not cause the optically isolated current detector on the base station to exceed its maximum current rating.

5.2.6
Remote Site Router – Connections

The site can be set up to benefit from the zone core redundancy afforded by a Dynamic System Resilience (DSR) configuration, or designed to connect to one zone core only as in systems without DSR.

- If the site is set up not to use DSR, the connections are made from the site router(s) to one zone core only.
- If the site is set up to use DSR, the connections are made to both primary and backup zone cores.

NOTICE: Contact your system administrator or see your customized system configuration plan for site router port connections in a Dynamic System Resilience configuration. For detailed information on the Dynamic System Resilience configuration, see the *Dynamic System Resilience Feature Guide* manual in this documentation set.

5.2.7 HPD Remote Site Router Connectors

The HPD site router connectors depend on a site function.

Table 52: HPD Remote Site Router Connectors

If the site:	Then the HPD remote site router requires:
Does not have circuit-based Conventional channels	• A T1/E1 I/O module (ST2512) • RJ-45 connectors
Has circuit-based Conventional channels	• A FlexWAN I/O module (ST2511) • FlexWAN serial connectors
Supports analog conventional channels	• Analog Conventional-to-IP Interface Kit (ST2513) • RJ-45 (analog) connectors
Supports digital conventional channels	• ASTRO® 25 Digital Conventional-to-IP Interface Kit (V.24 module, ST2514) • RJ-45 (digital) connectors

5.2.8 HPD Remote Site Router Cabling

A channel bank is installed as part of the subsystem only if circuit-based Conventional channels are required at the geographical site. Circuit-based Conventional channel audio can use the same transport facilities (T1 or E1) as the ASTRO® 25 system, but it is not processed by the IP components in the network. The IP-based devices in the system are not aware of the existence of circuit-based Conventional channel audio. The channel bank also connects to a FlexWAN port on the HPD remote site router(s) to transport voice and network management data IP packets to and from the master site.

The LAN port on the HPD remote site router connects to a port, which is labeled "Router" on the HPD site controller module. The site has two HPD site controller modules. One HPD remote site router at the site connects to "Router" port on the first HPD site controller module. If a second HPD remote site router is at the site, that router connects to the "Router" port on the second HPD site controller module.

The following table provides a list of connections to the HPD remote site routers at an HPD remote site.

Table 53: HPD Remote Site Router – HPD Site Controller A – Internal LAN Switch Connection Cable Connections

From Router		To Destination Device		
Port	Connector type	Device	Connector type	Description
LAN 1	RJ-45	Router A port, HPD Site Controller A	RJ-45	• If a standalone site controller is at the site, then the connection is made to the HPD remote site router port on the Site Controller A module (on its internal switch).

From Router		To Destination Device		
Port	**Connector type**	**Device**	**Connector type**	**Description**
				• If a site subsystem or expandable site subsystem is used at the site, then this connection is made to the HPD remote site router A port on the junction panel.
T1/E1	RJ-45	T1/E1, Primary Site Link	RJ-45	Connection to the site link (or CSU/DSU).
Ethernet module (Port 2) (if using Flexible Ethernet Site Links)	RJ-45	Ethernet backbone	RJ-45	This link exists between the router and the Ethernet backbone. Ethernet module (ST2510) must be installed in slot A of the S2500 router to make this connection for Flexible Ethernet links.
4-wire E&M ports	RJ-45	Conventional base station (optional)	RJ-45 (or other plus adapter)	If IP-based analog conventional channel stations are colocated at the site, up to four stations may be connected to an optional analog 4-wire E&M module in the HPD remote site router. See the conventional base station documentation for connection requirements.
60-pin FlexWAN		Channel bank (optional)	60-pin FlexWAN	If circuit-based Conventional channel equipment is at the site, then a V35 FlexWAN connection can be made to a channel bank to support the circuit-based equipment.
LAN 1	RJ-45	Router B port, HPD Site Controller B	RJ-45	The secondary HPD remote site router and its connections are only required if redundant site links are installed at the site. • If a standalone site controller is at the site, then the connection is made to the HPD remote site router port on the Site Controller B module (on its internal switch). • If a site subsystem or expandable site subsystem is used at the site, then this connection is made to the HPD remote site router, B port on the junction panel.
T1/E1	RJ-45	T1/E1, Backup Site Link	RJ-45	Connection to the secondary/backup site link (or CSU/DSU).
Ethernet module (Port 2) (if using Flexible Ethernet Site Links)	RJ-45	Ethernet backbone	RJ-45	This link exists between the router and the Ethernet backbone. Ethernet module (ST2510) must be installed in slot A of the S2500 router to

From Router		**To Destination Device**		
Port	**Connector type**	**Device**	**Connector type**	**Description**
				make this connection for Flexible Ethernet links.
4-wire E&M ports	RJ-45	Conventional base station	RJ-45 (or other plus adapter)	If IP-based analog conventional channel stations are colocated at the site, up to four stations may be connected (optional analog 4-wire E&M module required in the HPD remote site router).
V.24 module	RJ-45	Depends on the device being connected to the Digital CCGW	RJ-45	ASTRO® 25 Digital Conventional-to-IP Interface Kit (ST2514)

Table 54: HPD Remote Site Router – HPD Site Controller B – Internal LAN Switch Connection Cable Connections

From Router		**To Destination Device**		
Port	**Connector type**	**Device**	**Connector type**	**Description**
LAN 1	RJ-45	Router B port, HPD Site Controller B	RJ-45	The secondary HPD remote site router and its connections are only required if redundant site links are installed at the site. • If a standalone site controller is at the site, then the connection is made to the HPD remote site router port on the Site Controller B module (on its internal switch). • If a site subsystem or expandable site subsystem is used at the site, then this connection is made to the HPD remote site router, B port on the junction panel.
T1/E1	RJ-45	T1/E1, Backup Site Link	RJ-45	Connection to the secondary/backup site link (or CSU/DSU).
Ethernet module (Port 2) (if using Flexible Ethernet Site Links)	RJ-45	Ethernet backbone	RJ-45	This link exists between the router and the Ethernet backbone. Ethernet module (ST2510) must be installed in slot A of the S2500 router to make this connection for Flexible Ethernet links.
4-wire E&M ports	RJ-45	Conventional base station	RJ-45 (or other plus adapter)	If IP-based analog conventional channel stations are colocated at the site, up to four stations may be connected (optional analog 4-wire E&M module required in the HPD remote site router).

From Router		To Destination Device		
Port	**Connector type**	**Device**	**Connector type**	**Description**
V.24 module	RJ-45	Depends on the device being connected to the Digital CCGW	RJ-45	ASTRO® 25 Digital Conventional-to-IP Interface Kit (ST2514)

5.3

HPD Site Router – Maintenance and Troubleshooting

Generic maintenance and troubleshooting procedures apply. For maintenance and troubleshooting information, refer to S2500 Introduction, Installation, and Configuration on page 66.

Chapter 6

ASTRO 25 Dispatch Console Subsystem

This chapter provides information on the routers in an ASTRO® 25 system Dispatch Console subsystem, where different routers are used for different bandwidths.

6.1 Console Site Router (S6000)

Use the S6000 router, if the MCC 7500 Dispatch Console site requires more bandwidth than a T1 or E1,

6.1.1 Console Site Router – Functional Description

The Dispatch Console Site Subsystem router is required at console sites that are remote from the system's zone core.

Depending on the bandwidth required by the console site, the following router models are used:

- Motorola Network Router (MNR) S2500 routers or GGM 8000 Gateways
- Motorola Network Router (MNR) S6000 routers

A remote console site may have redundant or non-redundant links to the zone core.

- If the site implements one T1/E1 network link to the core, a single console site router is used to make the physical connection to the core router.
- If redundant T1/E1 links are implemented, two console site routers are used.
- If Ethernet Site links are used, the console site must use an S6000 router as this implementation requires three Ethernet ports to support Ethernet Site Links.
- If the Console Site implements hybrid redundant site links, T1/E1 can be employed for one site link while Ethernet can be employed for the other site link. See Hybrid Site Link Overview on page 121.

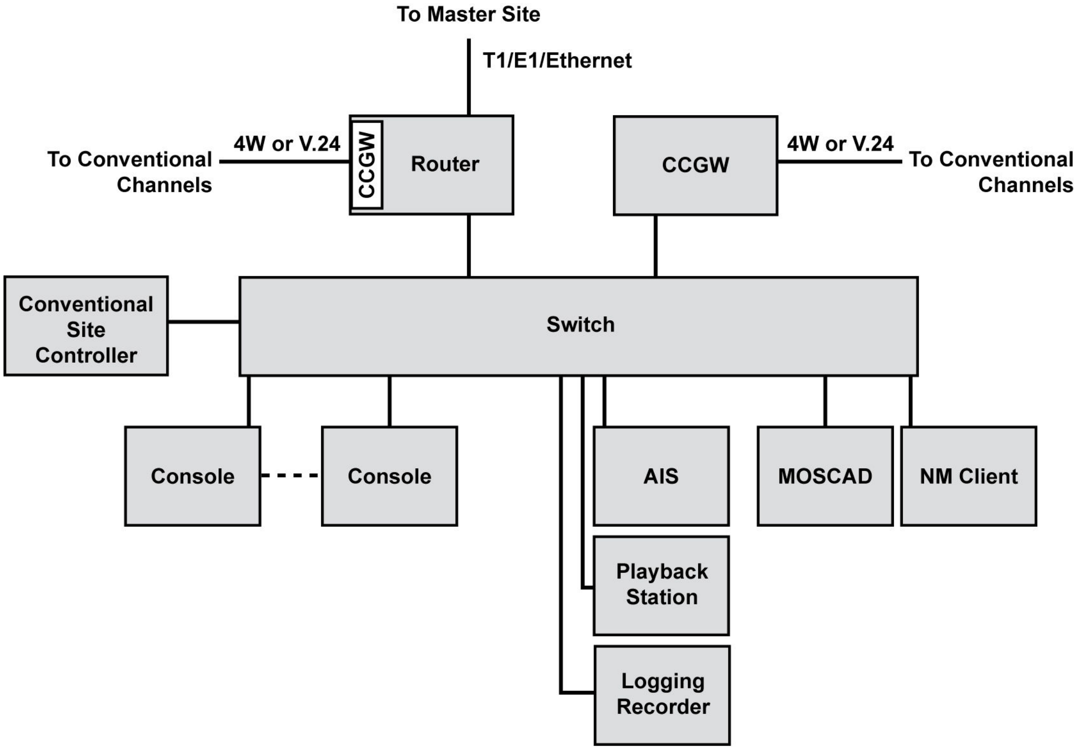
See the *Flexible Site and InterZone Links* manual for details.

Console site routers can also host conventional channels if they include the V.24 (for digital connectivity) or E&M modules (for analog connectivity). See the Conventional Channel Gateway (CCGW) on page 212 for details.

NOTICE: The S2500 router is not compatible with MDC-1200 channels, IP conventional channels, or the increased key strength feature. If these features are used on the system, the GGM 8000 Gateway must be employed. Refer to the *GGM 8000 System Gateway* manual for details.

If the MCC 7500 Dispatch Console site is remote, the interface to the system is similar to an RF Site Link. In a remote site, there is a WAN link from the zone core to the console site. Depending on whether the WAN link is redundant, the MCC 7500 Dispatch Console site requires one or two site routers.

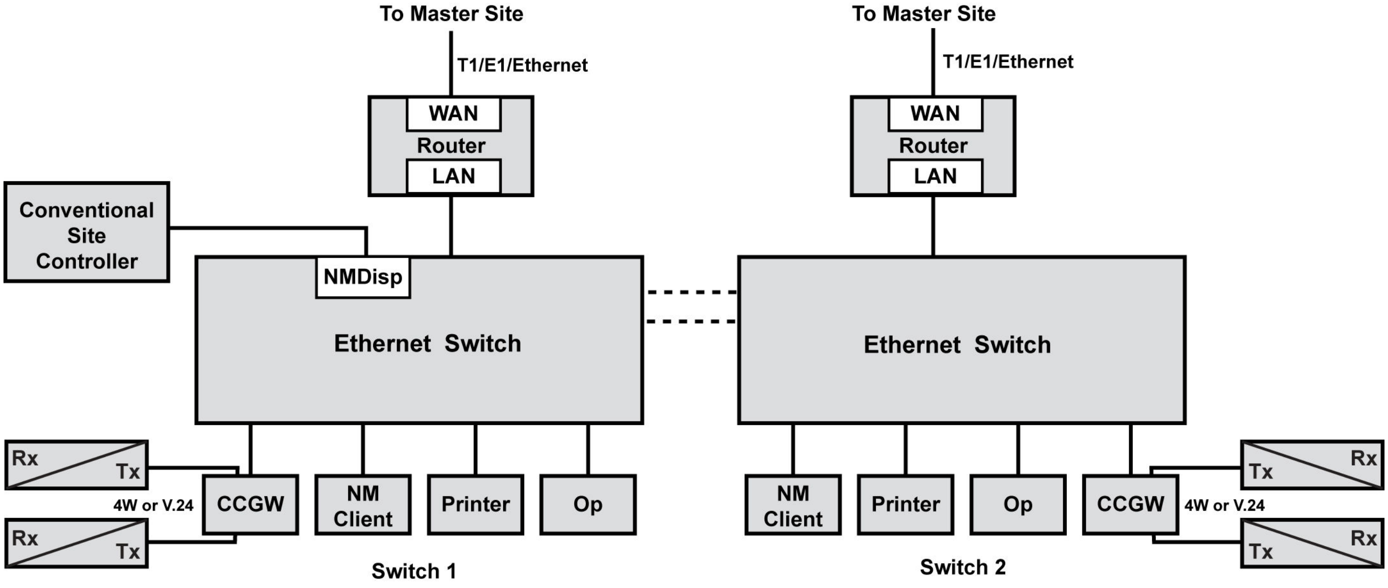
Figure 41: MCC 7500 Remote Console Site Block Diagram



conv_remote_console_config_single1

The following figure shows the architecture for a console site with colocated conventional that has dual site links. If the bandwidth needs call for multiple T1s/E1s, the S6000 router must be used.

Figure 42: Console Site with Colocated Conventional with Dual Site Links



conv_remote_console_config_dual1

6.1.2 Console Site Router (S6000) – Installation and Configuration

Prerequisites: Ensure that you have the required cabling and connectors.

Process:

1. Install the console site router in a rack. See S6000 Introduction, Installation, and Configuration on page 27.
2. Connect the console site router to a power source. See S6000 Introduction, Installation, and Configuration on page 27.
3. If necessary, ground the console site router. See S6000 Introduction, Installation, and Configuration on page 27.
4. Connect the CEN equipment to the console site router. See Console Site Router (S6000) Cabling on page 159.
5. Configure the console site router. See S6000 Introduction, Installation, and Configuration on page 27.

6.1.2.1 Console Site Router (S6000) Cabling

Table 55: Console Site Router Cable Connections

From Console Site Router		**To Destination Device**		
Port	Connector Type	Port	Connector Type	Description
LAN 1	RJ45	Port 1, Prime Site Switch 1	RJ45	Connection to the prime site switch
Port 5B	T1/E1, UltraWAN/ RJ48c	T1 or E1 from carrier	T1/E1, UltraWAN/ RJ48c	T1/E1 connection to master site
Port 5C	T1/E1, UltraWAN/ RJ48c	T1 or E1 from carrier	T1/E1, UltraWAN/ RJ48c	T1/E1 connection to master site
Port 5D	T1/E1, UltraWAN/ RJ48c	T1 or E1 from carrier	T1/E1, UltraWAN/ RJ48c	T1/E1 connection to master site

6.1.3 Console Site Router (S6000) – Maintenance and Troubleshooting

Generic maintenance and troubleshooting procedures apply. For maintenance and troubleshooting information, refer to S6000 Introduction, Installation, and Configuration on page 27.

6.2 Console Site Router (S2500)

MCC 7500 Dispatch console sites that need a single T1 or E1 of bandwidth or less may be installed with S2500 routers regardless of whether they have redundant site links.

6.2.1 Console Site Router – Functional Description

The Dispatch Console Site Subsystem router is required at console sites that are remote from the system's zone core.

Depending on the bandwidth required by the console site, the following router models are used:

- Motorola Network Router (MNR) S2500 routers or GGM 8000 Gateways
- Motorola Network Router (MNR) S6000 routers

A remote console site may have redundant or non-redundant links to the zone core.

- If the site implements one T1/E1 network link to the core, a single console site router is used to make the physical connection to the core router.
- If redundant T1/E1 links are implemented, two console site routers are used.
- If Ethernet Site links are used, the console site must use an S6000 router as this implementation requires three Ethernet ports to support Ethernet Site Links.
- If the Console Site implements hybrid redundant site links, T1/E1 can be employed for one site link while Ethernet can be employed for the other site link. See Hybrid Site Link Overview on page 121.

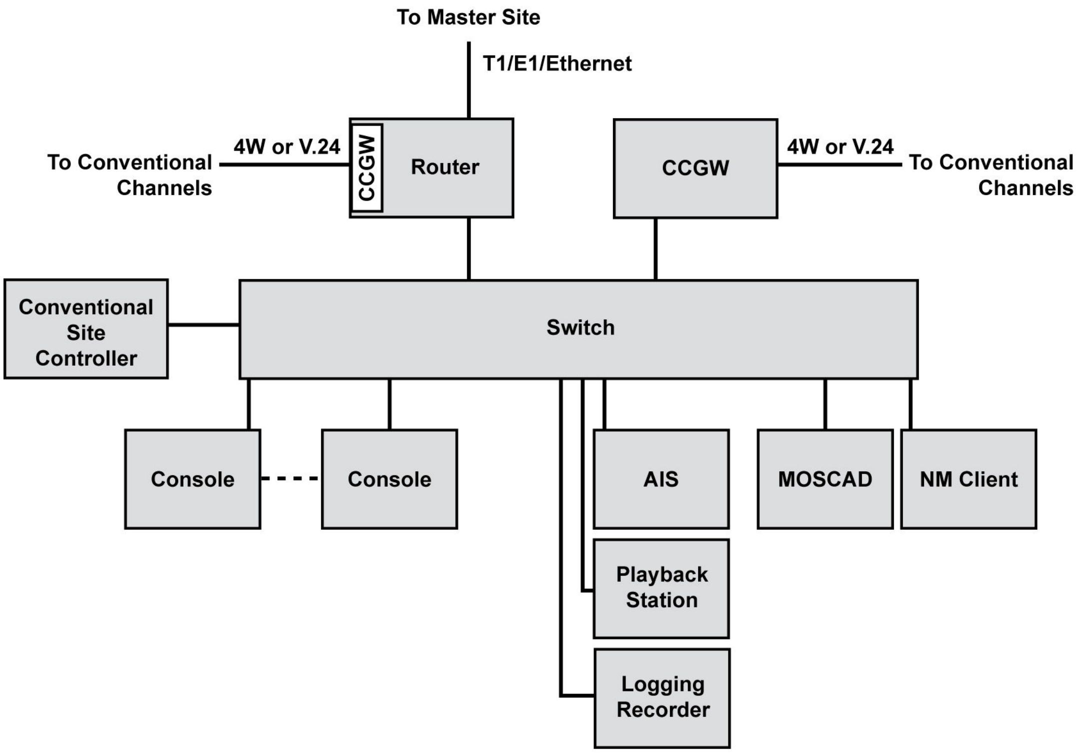
See the *Flexible Site and InterZone Links* manual for details.

Console site routers can also host conventional channels if they include the V.24 (for digital connectivity) or E&M modules (for analog connectivity). See the Conventional Channel Gateway (CCGW) on page 212 for details.

NOTICE: The S2500 router is not compatible with MDC-1200 channels, IP conventional channels, or the increased key strength feature. If these features are used on the system, the GGM 8000 Gateway must be employed. Refer to the *GGM 8000 System Gateway* manual for details.

If the MCC 7500 Dispatch Console site is remote, the interface to the system is similar to an RF Site Link. In a remote site, there is a WAN link from the zone core to the console site. Depending on whether the WAN link is redundant, the MCC 7500 Dispatch Console site requires one or two site routers.

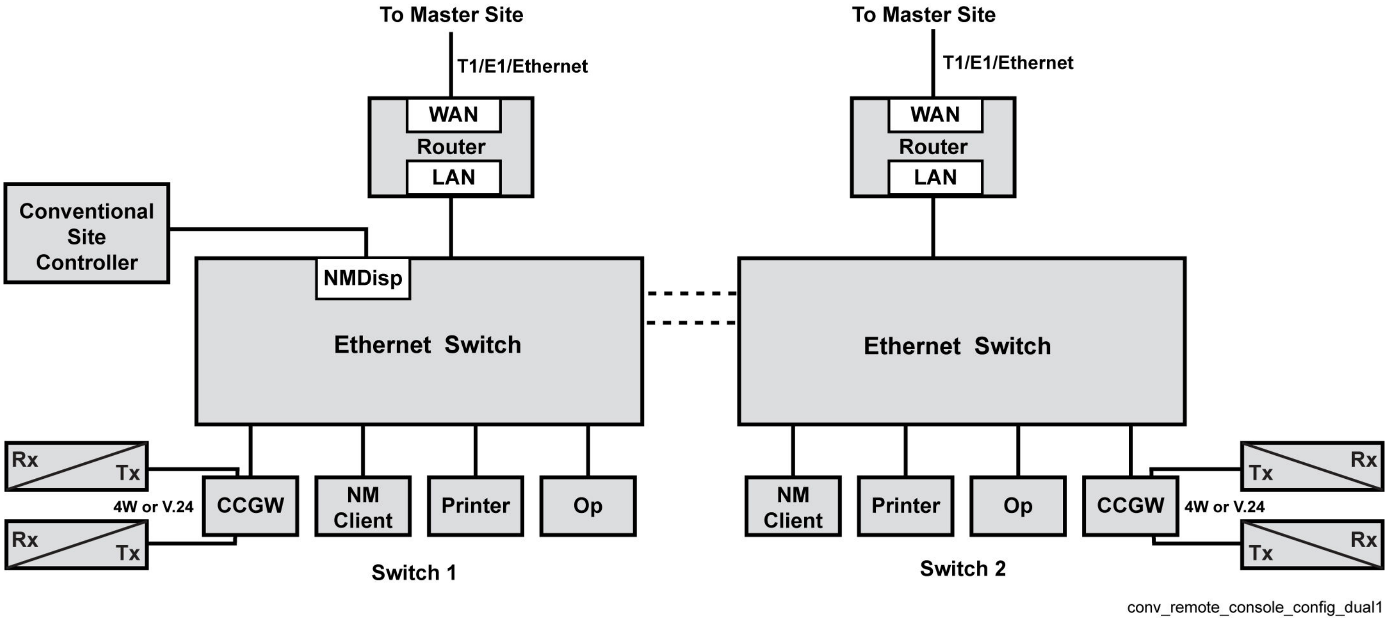
Figure 43: MCC 7500 Remote Console Site Block Diagram



conv_remote_console_config_single1

The following figure shows the architecture for a console site with colocated conventional that has dual site links. If the bandwidth needs call for multiple T1s/E1s, the S6000 router must be used.

Figure 44: Console Site with Colocated Conventional with Dual Site Links



6.2.2

Console Site Router (S2500) – Installation and Configuration

Prerequisites: Prepare the required cabling and connectors.

Process:

1. Install the console site router in a rack. See S2500 Introduction, Installation, and Configuration on page 66.
2. Connect the console site router to a power source. See S2500 Introduction, Installation, and Configuration on page 66.
3. If necessary, ground the console site router. See S2500 Introduction, Installation, and Configuration on page 66.
4. Connect the equipment to the console site router. See Console Site Router (S2500) Cabling on page 161.
5. Configure the console site router. See S2500 Introduction, Installation, and Configuration on page 66.

6.2.2.1

Console Site Router (S2500) Cabling

The following table lists generic connections between the site router and other devices at the remote site.

Table 56: Console Site Router Cable Connections

From Router		To Destination Device		
Port	**Connector type**	**Port**	**Connector type**	**Description**
LAN 1	RJ-45	Port 1, Ethernet LAN Switch	RJ-45	Communications connection between the

From Router		To Destination Device		
Port	Connector type	Port	Connector type	Description
				S2500 console site router and the Ethernet LAN switch.
I/O Module A (T1/E1)	RJ-45	T1 or E1 from carrier	RJ-45	This T1/E1 link connects the console site through the router to the master site. The T1/E1 I/O module (ST2512) must be installed in the S2500 to make this connection.

NOTICE: Refer to the customized cabling and configuration information provided by Motorola Solutions for port connections specific to your system.

6.2.3 Console Site Router (S2500) – Maintenance and Troubleshooting

Generic maintenance and troubleshooting applies. For maintenance and troubleshooting information, see S2500 Introduction, Installation, and Configuration on page 66.

Chapter 7

ASTRO 25 IP Simulcast Subsystem

This chapter provides information on the routers in an ASTRO® 25 IP Simulcast subsystem.

7.1 IP Simulcast Subsystem Prime Site Router

The IP Simulcast Prime Site router handles the traffic between the prime site network and the master site.

7.1.1 IP Simulcast Prime Site Routers – Functional Description

Two S6000 router serves two functions at the prime site.

S6000 prime site router

The router handles the traffic between the prime site network and the master site. The prime site router distributes voice, control, and network management traffic to the appropriate devices on the prime site network.

Remote Site Access router

It is the interface between the prime site router and the remote site router. The remote site access router interfaces to the prime site router through its Ethernet LAN port and connects to the remote site router through a WAN Link. There are two types of WAN links used for connecting to the remote site routers: Ethernet and T1/E1 links. For T1/E1 links, the access router requires a 12-port module in a Cooperative WAN Routing (CWR) arrangement. For Geographically Redundant Prime Sites, it requires Ethernet links only.

NOTICE: For additional information on the IP simulcast prime site as a whole, see the *Trunked IP Simulcast Subsystem Prime Site* manual. If the prime site routers and remote site access routers are configured for encryption, see the *Link Encryption and Authentication* manual for details about installation and configuration issues specific to router encryption.

7.1.1.1 Prime Site Router – Function

The prime site router directs all control, voice, and network management traffic between the prime site LAN and the site link to the master site. The router connects to T1/E1 links through UltraWAN ports and connects to Ethernet links through a LAN port. An optional redundant prime site router can be installed in the prime site.

The site can be set up to benefit from the zone core redundancy afforded by Dynamic System Resilience (DSR), or designed to connect to one zone core only as in systems without DSR. For detailed information on the DSR configuration, see the *Dynamic System Resilience Feature Guide* manual.

If a Geographically Redundant Prime Site configuration is present in the system, two prime site routers are required: the Primary and Secondary Prime Site Router.

The S6000 router with an ST6010 UltraWAN module or ST6017 UltraWAN II is used as the prime site router.

The prime site routers functions are:

Media conversion

The router converts the 100 MB Ethernet LAN packets to IP packets encapsulated in Frame Relay on a serial WAN interface or to tunneled IP packets on an Ethernet flexible site link.

Traffic prioritizing

The router applies the correct prioritization masking to the packets leaving the site.

Fragmentation

The router fragments large IP packets per standards.

Dynamic Host Configuration Protocol (DHCP) service

This service allows the technician to connect to the LAN at the site using a properly configured PC with the Windows OS.

The prime site router is based on the Motorola Network Router (MNR) S6000. Three built-in Ethernet ports (LAN ports) provide connectivity to the site Ethernet switch, where both the primary site controller and the backup site controller are accessible. If circuit-based Conventional channels are present, the UltraWAN module (ST6010) or UltraWAN II module (ST6017) provides either a T1 or E1 interface to the TeNSr channel bank WAN card.

NOTICE: The S6000 router supports two versions of the UltraWAN module. The functionality of the two module versions is the same; however, the UltraWAN II module (identified by a Roman numeral “II” on the front panel), requires EOS software version 15.4 or higher.

CAUTION: If you install an UltraWAN II module in an S6000 running a version of EOS software lower than the required version, the router reboots continuously.

The prime site router facilitates network management activity at the site and provides a medium for receiving and reporting failure alarms. The Unified Network Configurator (UNC), Unified Event Manager (UEM), and MOSCAD Network Fault Management (NFM) have access to the simulcast prime site and remote site through the prime site router and remote site access router.

7.1.1.2
Prime Site to Master Site Links

A link is defined as both the physical and logical connections between two entities. The link type used in a prime site to master site connection is called a site link.

Table 57: Prime Site to Master Site Link Type

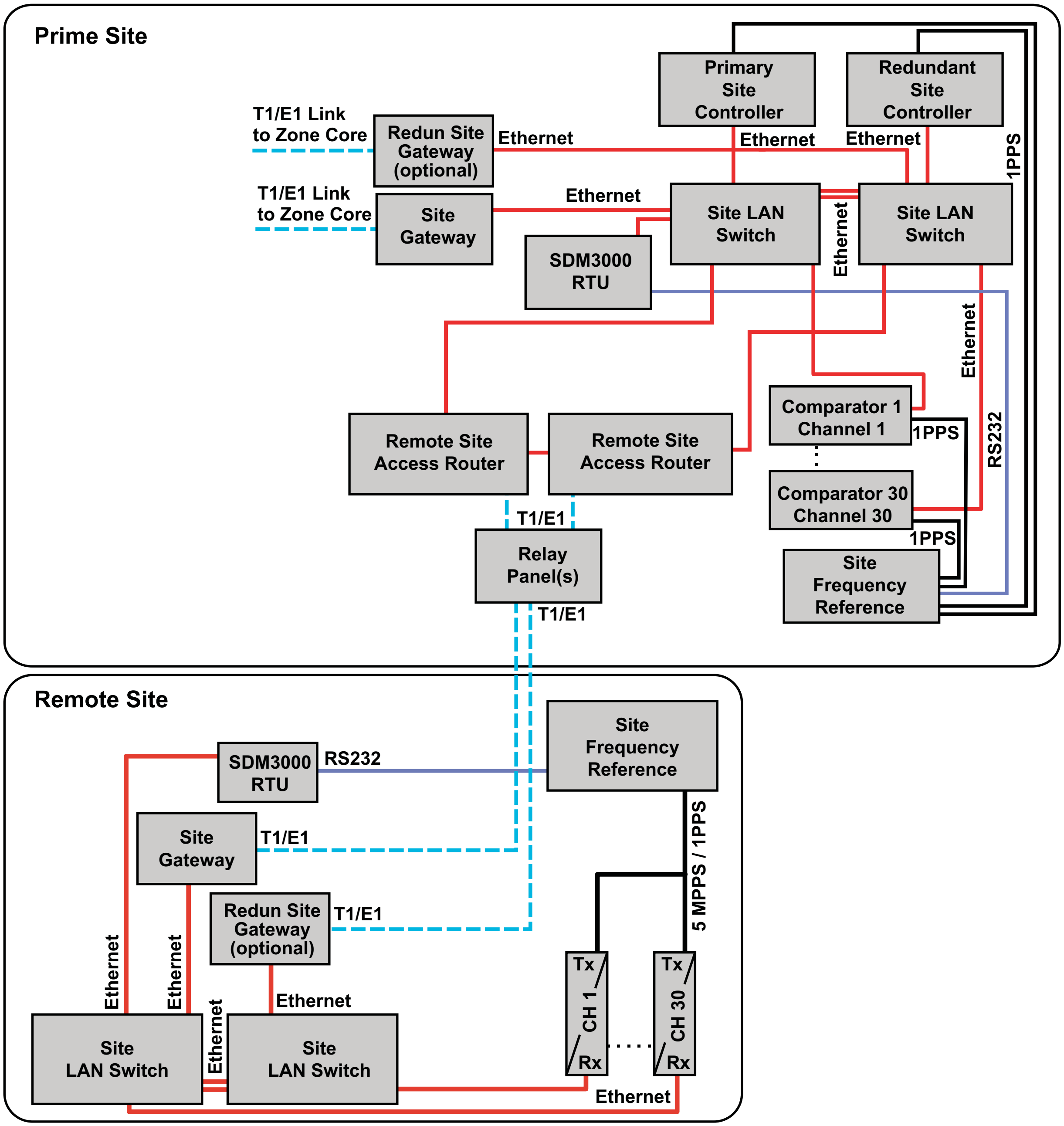
Link Name	Physical Description	Logical Description
Site Link	Connects the master site and prime site. Fractional T1 (FT1) or T1 between the WAN switch/CWR relay panel at the master site and prime site router. Bandwidth may range from 384 K up to T1/E1 depending on the channels and/or encryption.	Provides the physical connection between the redundant core routers at the master site and prime site router. The physical connection is used to set up the logical links. Logical path is through redundant frame relay Permanent Virtual Circuits (PVCs). Control traffic uses both PVCs. All other traffic, including audio, uses one of the PVCs.

The IP simulcast subsystem allows for a single site link and dual site links between prime and master sites. For more information, see Figure 47: Single Site Link between Prime Site and Master Site on page 167 and Figure 48: Dual Site Links between Prime Site and Master Site on page 167.

Figure 45: Single or Dual Site Links of the Prime Site on page 165 shows a representative prime site configuration with a single and a redundant prime site router link (optional) going to the master site.

NOTICE: Single Site Links between Prime Site and Master Site do not apply to systems with a Geographically Redundant Prime Site configuration. Dual site links are present in those systems. See Figure 46: Dual Site Links of the Prime Site (Geographically Redundant Prime Sites) on page 166.

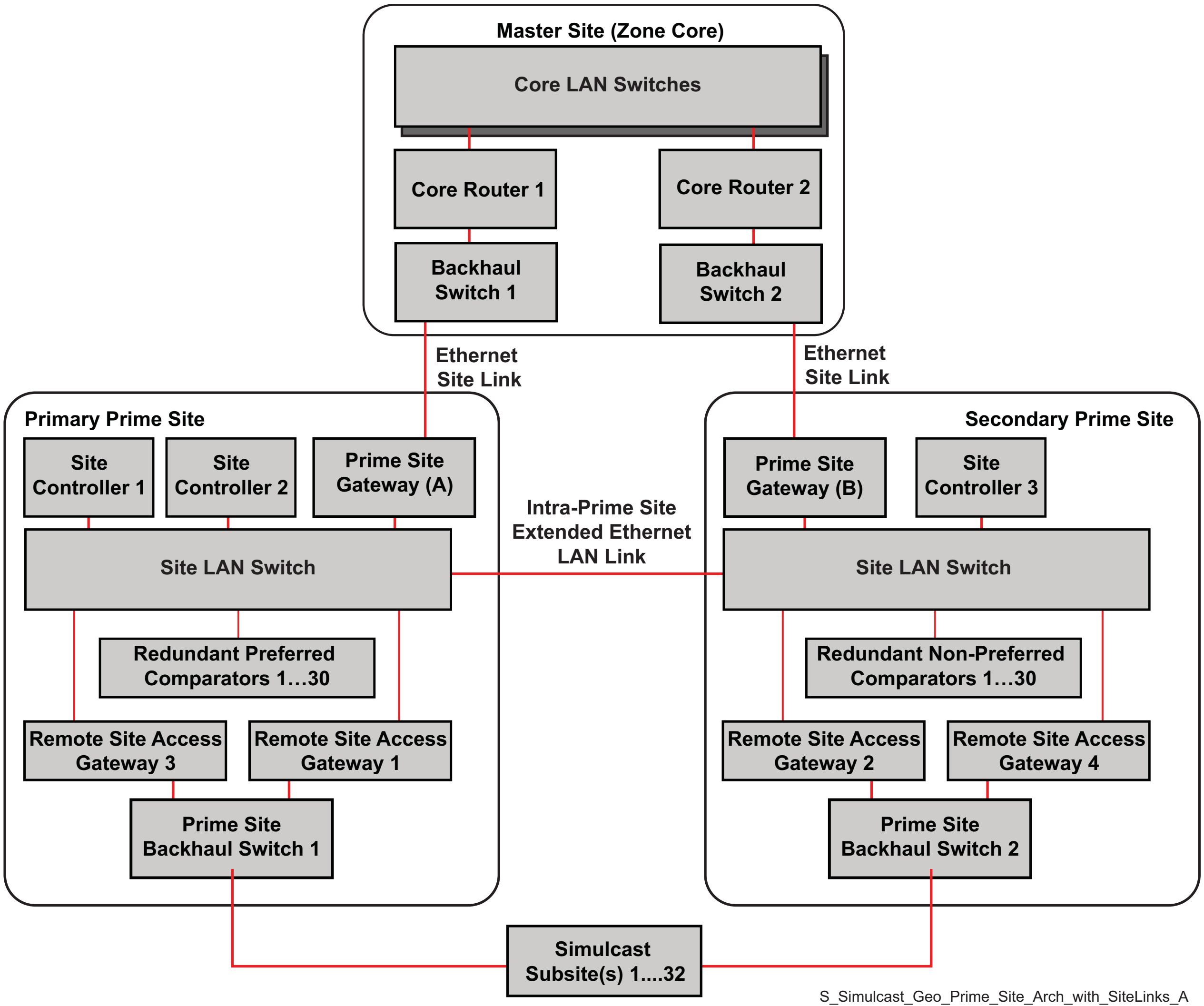
Figure 45: Single or Dual Site Links of the Prime Site



S_IP_Simul_Subsystem_T1E1_Site_Link_D

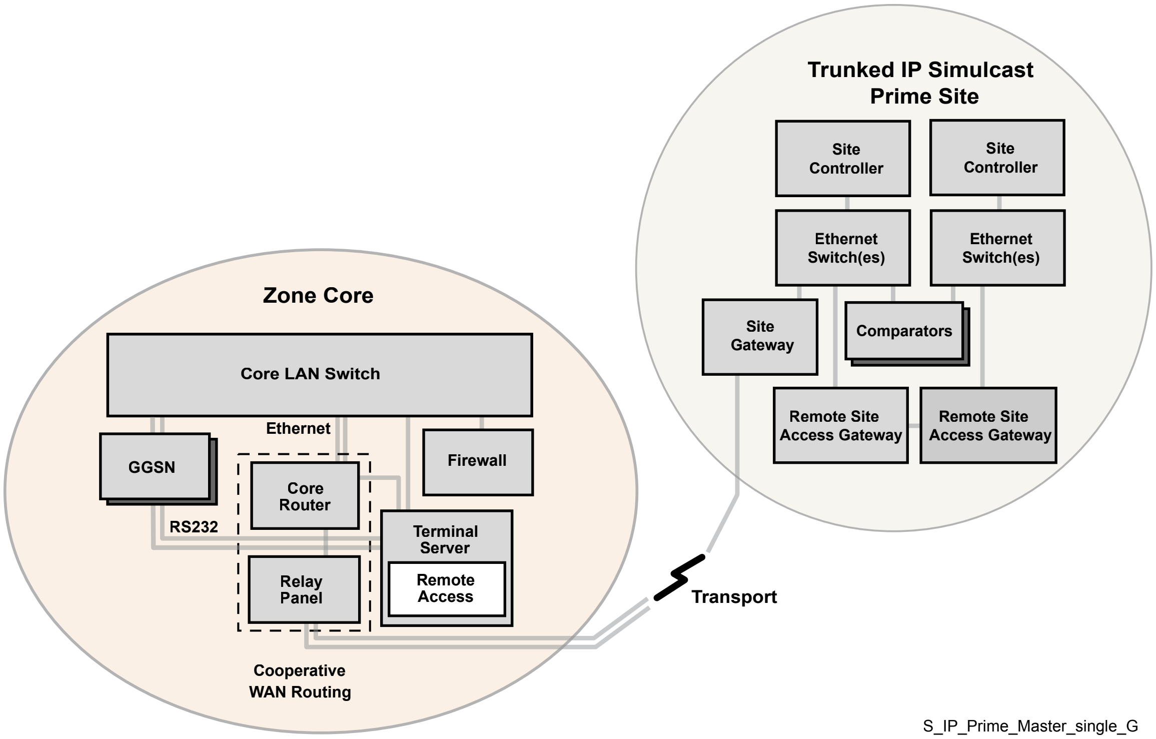
NOTICE: The redundant prime site router (optional) in the diagram, is not included in a single router link configuration to the master site.

Figure 46: Dual Site Links of the Prime Site (Geographically Redundant Prime Sites)


Master Site (Zone Core)
Core LAN Switches
Core Router 1
Core Router 2
Backhaul Switch 1
Backhaul Switch 2
Ethernet Site Link
Ethernet Site Link
Primary Prime Site
Site Controller 1
Site Controller 2
Prime Site Gateway (A)
Site LAN Switch
Redundant Preferred Comparators 1…30
Remote Site Access Gateway 3
Remote Site Access Gateway 1
Prime Site Backhaul Switch 1
Intra-Prime Site Extended Ethernet LAN Link
Secondary Prime Site
Prime Site Gateway (B)
Site Controller 3
Site LAN Switch
Redundant Non-Preferred Comparators 1…30
Remote Site Access Gateway 2
Remote Site Access Gateway 4
Prime Site Backhaul Switch 2
Simulcast Subsite(s) 1....32

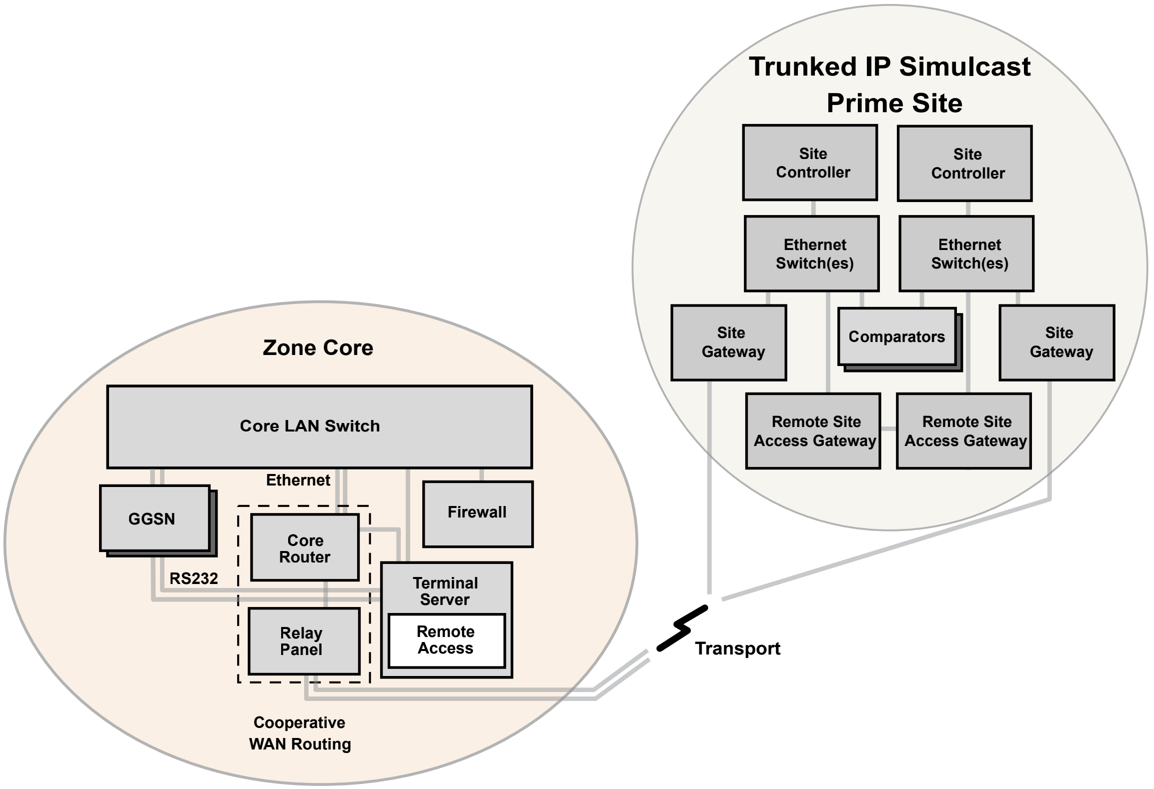
S_Simulcast_Geo_Prime_Site_Arch_with_SiteLinks_A

Figure 47: Single Site Link between Prime Site and Master Site



S_IP_Prime_Master_single_G

Figure 48: Dual Site Links between Prime Site and Master Site



S_IP_Prime_Master_dual_G

NOTICE: If Dynamic System Resilience is implemented on your system, refer to the *Dynamic System Resilience* manual for details on connections and diagrams relating to the prime site router.
For redundant Prime Site to Master Site links, hybrid redundant site links can be employed. See Hybrid Site Link Overview on page 121.

7.1.1.3
Prime Site to Remote Sites Link

A link is defined as both the physical and logical connections between two entities. The link type used in a prime site to remote site connection is called a site link.

Table 58: Prime Site to Remote Sites Link Type

Link Name	Physical Description	Logical Description
Remote Site Link	Connects the prime site to the remote site through the remote site access routers.	Provides the physical connection, which is used to create the logical connection between the remote site's IP links to the comparators at the prime site.

7.1.1.4
Prime Site Router Connections

The prime site router has an UltraWAN port and a LAN ports. The UltraWAN port supports a T1/E1 link to the master site. The LAN ports support an Ethernet link to the master site and an Ethernet connection to the prime site LAN. See Figure 49: IP Simulcast Subsystem Prime Site on page 169.

The Outbound Multi-frame relay traffic from the master site is carried over a Permanent Virtual Circuit (PVC) to the prime site router. The prime site router terminates the PVC and Multi-frame relay, and then distributes audio and control traffic to the prime site LAN, where it is processed by the site controllers or comparators.

The audio and control traffic intended for the zone core is sent to the prime site router over the prime site LAN. The prime site router encapsulates the traffic into Multi-frame relay and delivers the traffic over the T1/E1 or Ethernet link to the master site.

The prime site can be set up to benefit from the zone core redundancy afforded by Dynamic System Resilience (DSR), or designed to connect to one zone core only as in systems without DSR.

- If the prime site is set up not to use DSR, the connections are made from the site router(s) to one zone core only.
- If the prime site is set up to use DSR, the connections are made to both primary and backup zone cores.

NOTICE: Contact your system administrator or see your customized system configuration plan for prime site router port connections in a DSR scenario. For detailed information on a Dynamic System Resilience configuration, see the *Dynamic System Resilience Feature Guide* manual.

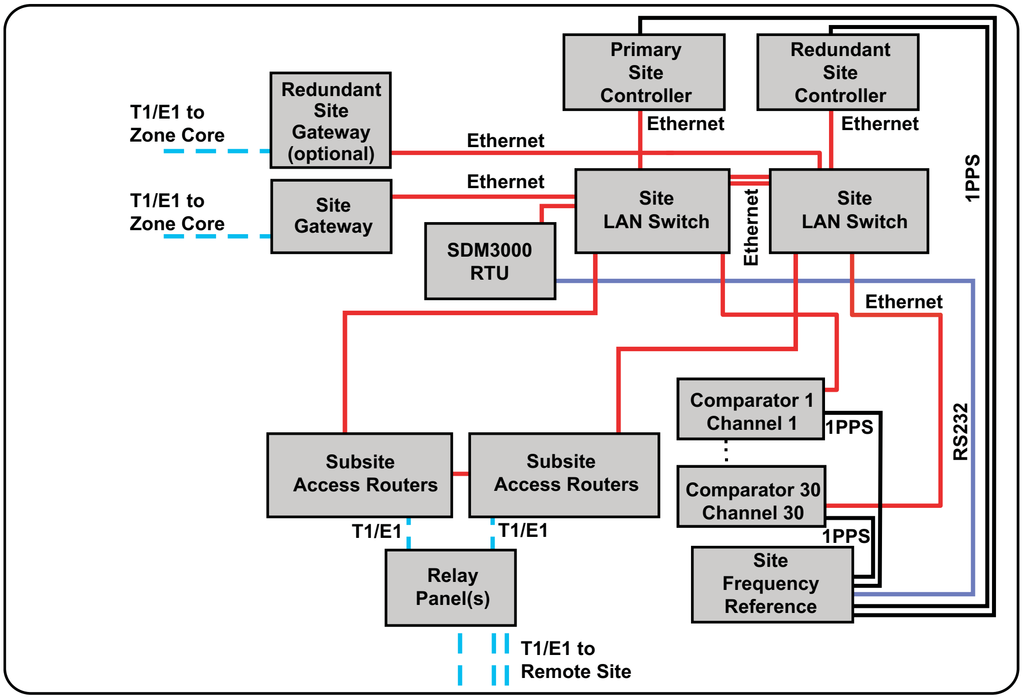
If circuit-based Conventional channels are supported in the subsystem, the site configuration is slightly different. The prime site router delivers frame relay traffic over T1/E1 through the channel bank, which multiplexes the circuit-based Conventional channels and traffic into separate timeslots and delivers the channelized T1/E1 to the master site.

If a Geographically Redundant Prime Site configuration is present in the system, two prime site routers are required: the Primary and Secondary Prime Site Router.

Table 59: Port Connections for the Prime Site Routers

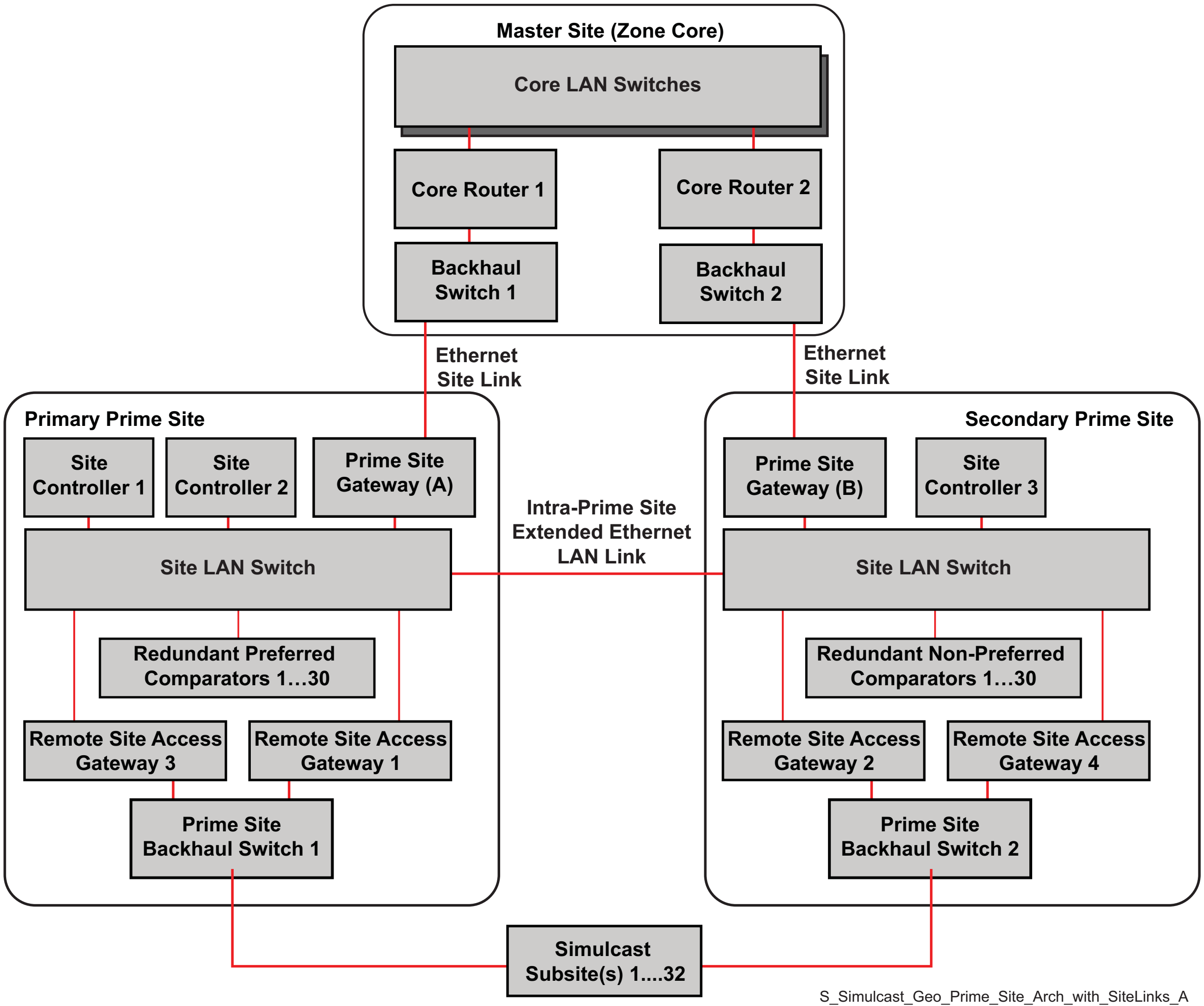
Port	Destination
Prime Site Router 1	
LAN 1	Prime Site Switch 1
T1/E1 or LAN 3	Ethernet WAN link to the zone core
5A-5C	T1/E1 connection to the zone core
Prime Site Router 2	
LAN 1	Prime Site Switch 2
T1/E1 or LAN 3	Ethernet WAN link to the zone core
5A-5C	T1/E1 connection to the zone core

Figure 49: IP Simulcast Subsystem Prime Site



S_IP_Simul_Prime_Site_E

Figure 50: IP Simulcast Subsystem Geographically Redundant Prime Sites


Master Site (Zone Core)
Core LAN Switches
Core Router 1
Core Router 2
Backhaul Switch 1
Backhaul Switch 2
Ethernet Site Link
Ethernet Site Link
Primary Prime Site
Site Controller 1
Site Controller 2
Prime Site Gateway (A)
Site LAN Switch
Redundant Preferred Comparators 1…30
Remote Site Access Gateway 3
Remote Site Access Gateway 1
Prime Site Backhaul Switch 1
Intra-Prime Site Extended Ethernet LAN Link
Secondary Prime Site
Prime Site Gateway (B)
Site Controller 3
Site LAN Switch
Redundant Non-Preferred Comparators 1…30
Remote Site Access Gateway 2
Remote Site Access Gateway 4
Prime Site Backhaul Switch 2
Simulcast Subsite(s) 1....32

S_Simulcast_Geo_Prime_Site_Arch_with_SiteLinks_A

NOTICE: For information on Ethernet connectivity between the sites and zones, see the *Flexible Site and InterZone Links* manual.
Ethernet site links are used for connecting to Geographically Redundant Prime Sites.

7.1.1.5
Prime Site Router – EOS Functions

A certain list of interfaces, protocols, basic routing, and IP features in the Enterprise OS (EOS) is used by the prime site router.

The prime site router uses basic routing and IP features in the Enterprise OS (EOS) software including the following:

- IP Routing
- 10/100 Ethernet
- Channelized T1
- Static Routes
- Multi-frame Relay
- Fragmentation

- Flexible Ethernet Links

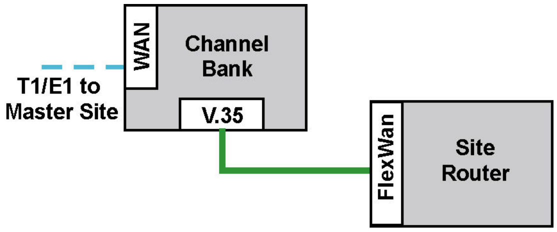
The prime site router uses the following protocols and interfaces:

- Simple Network Management Protocol (SNMP)
- Multicast
- Type of Service (TOS)
- Dynamic Host Configuration Protocol (DHCP)
- Network Time Protocol (NTP)

7.1.1.6 Circuit-Based Conventional Channels Overlay

An IP simulcast subsystem transport network may be overlaid with network transport for circuit-based Conventional channels, such as voted analog circuit-based Conventional channels or V.35-based digital channels. If circuit-based Conventional channels or digital channels are present, channel banks are required to multiplex the Conventional channels transport circuits and the IP traffic on the WAN links.

Figure 51: IP Simulcast Prime Site Router with Circuit-Based Conventional Channels Overlay Connections



IP_Simul_w_mutual_router_connec

7.1.2 IP Simulcast Prime Site Routers – Installation and Configuration

Prerequisites: Prepare the required cabling and connectors.

Process:

1. Install the IP Simulcast Prime Site Router in a rack. See S6000 Introduction, Installation, and Configuration on page 27.
2. Connect the IP Simulcast Prime Site Router to a power source. See S6000 Introduction, Installation, and Configuration on page 27.
3. If necessary, ground the IP Simulcast Prime Site Router. See S6000 Introduction, Installation, and Configuration on page 27.
4. Connect the equipment to the IP Simulcast Prime Site Router. See IP Simulcast Prime Site Router Cabling on page 172.
5. Configure the IP Simulcast Prime Site Router. See S6000 Introduction, Installation, and Configuration on page 27.

7.1.2.1
IP Simulcast Prime Site Router Cabling

This section describes how to cable each interface on the IP Simulcast Prime Site routers.

NOTICE: If a Dynamic System Resilience (DSR) configuration is implemented on your system, see Prime Site Router Connections on page 168 for details.

7.1.2.1.1
Cabling the Prime Site Router

Table 60: Cable Connections from the Prime Site Router

From Prime Site Router		Destination Device		
Port	**Connector Type**	**Port**	**Connector Type**	**Description**
LAN 1	RJ45	Port 1, Prime Site Switch 1	RJ45	Connection to the prime site switch
LAN 3	RJ45	Ethernet from carrier	RJ45	Ethernet WAN link to master site
Port 5B	T1/E1, UltraWAN/ RJ48c	T1 or E1 from carrier	T1/E1, UltraWAN/ RJ48c	T1/E1 connection to master site
Port 5C	T1/E1, UltraWAN/ RJ48c	T1 or E1 from carrier	T1/E1, UltraWAN/ RJ48c	T1/E1 connection to master site
Port 5D	T1/E1, UltraWAN/ RJ48c	T1 or E1 from carrier	T1/E1, UltraWAN/ RJ48c	T1/E1 connection to master site

NOTICE: If a redundant router is used, connect Port 1 and Port 2 to the corresponding ports on Switch 2.
A Channel bank is used in IP simulcast subsystem only when circuit-based Conventional channels are present.

7.1.2.2
Router Encryption Card Installation and Configuration

For more information, see the *Link Encryption and Authentication* manual.

7.1.3
IP Simulcast Prime Site Routers – Maintenance and Troubleshooting

Generic maintenance and troubleshooting procedures apply. For maintenance and troubleshooting information, see S6000 Introduction, Installation, and Configuration on page 27.

7.1.3.1
Router Encryption Card Troubleshooting

See the *Link Encryption and Authentication* manual for more information.

7.2
IP Simulcast Subsystem Remote Site Router

The IP Simulcast Remote Site router handles traffic between the remote site network and the T1 link to the prime site.

7.2.1 IP Simulcast Remote Site Router – Functional Description

The remote site router provides a Wide Area Network (WAN) interface that handles all of the traffic to and from the zone for the Radio Frequency (RF) site including voice, control, data, and network management traffic.

In a simulcast remote site, the remote site router transports the site network management information to and from the Unified Network Configurator (UNC), Unified Event Manager (UEM), and MOSCAD Network Fault Management (NFM) servers. The Local Area Network (LAN) port is connected to the Ethernet switch where the base radio and MOSCAD RTU are also connected.

The S2500 site router handles traffic between the remote site network and the T1 link to the prime site. The remote site router distributes network management traffic between the components on the remote site network.

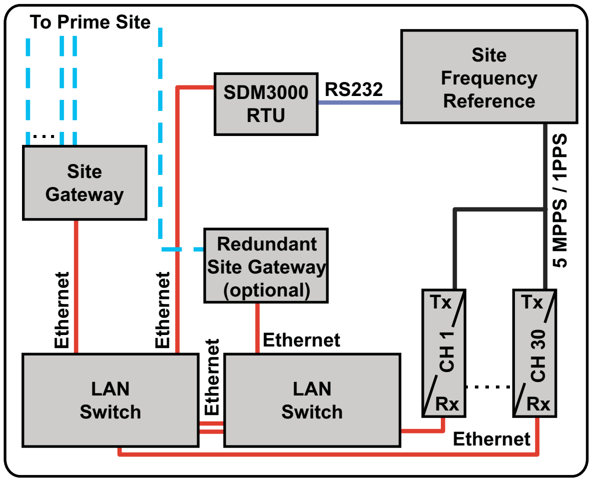
The remote site router integrates voice and data traffic over a single converged network, compressing and routing voice calls between devices directly connected to the switch or between telephones or Private Branch Exchange (PBX) through an IP data network.

The remote site router provides the IP network routing interface between the remote and the prime site. The remote site router connects to the prime site through the relay panels at the prime site. The relay panels then attach to the remote site access routers at the prime site. In the dual remote link configuration, two remote site routers are deployed, one for each remote link.

NOTICE: For additional information on the IP simulcast subsystem as a whole, see the *Trunked IP Simulcast Subsystem Remote Site* manual and the *Trunked IP Simulcast Subsystem Infrastructure* manual.

Typically, routers at the IP simulcast remote site interface with the components shown in the diagram below.

Figure 52: Remote Site – Connections



S_IP_Simul_Remote_Site_B

NOTICE: Ethernet site links are used for connecting to Geographically Redundant Prime Sites.

Remote site routers provide the following functions:

Media conversion
The router converts the 100 MB Ethernet LAN packets to IP packets encapsulated in Frame Relay on a serial WAN interface or to tunneled IP packets on an Ethernet flexible site link.

Traffic prioritizing
The router applies the correct prioritization masking to the packets leaving the site.

Fragmentation

The router fragments large IP packets as per standards.

Dynamic Host Configuration Protocol (DHCP) service

This service allows a technician to connect to the LAN at the site using a properly configured PC with the Windows OS.

Redundancy

There can be two routers at the remote site, which provide redundancy. While one of the routers is operational, the other router is redundant. This optional redundant remote site router along with the redundant links to the redundant router provides protection from single router failure or single WAN link failure.

NOTICE: Redundancy is an optional configuration.

7.2.1.1

IP Simulcast Remote Site Router I/O Modules Functions

At a remote site, the router is used to provide connectivity from the remote site LAN to the IP simulcast prime site controller, Unified Network Configurator (UNC), Unified Event Manager (UEM), and MOSCAD Network Fault Management (NFM) servers. The remote site router may also support Conventional Channel Gateway (CCGW) functionality to provide connectivity to analog conventional or ASTRO® 25 Conventional channel resources.

Table 61: IP Simulcast Remote Site Router Functional Description with I/O Modules

Functional Router Description	S2500 I/O Module Slot A Port 2	S2500 I/O Module Slot B Port 3	S2500 Analog Module Slot Ports 4, 5, 6, 7
Remote Site Router – Prime Site interface only	ST2512 T1/E1 module or ST2510* 10Base-T module For Geographically Redundant Prime Sites: 10Base-T module	Empty	Empty
Remote Site Router – Analog CCGW	ST2512 T1/E1 module or ST2510* 10Base-T module	Empty	ST2513 Conventional-to-IP Kit
Remote Site Router – Digital CCGW	ST2512 T1/E1 module or ST2510* 10Base-T module	ST2514 V.24 module	Empty or ST2513 Analog Conventional-to-IP Interface Kit
Remote Site Router – circuit-based Conventional channels support	Empty	ST2511 FlexWAN module	Empty
Remote Site Router – circuit-based Conventional channels support plus Analog CCGW	Empty or ST2514 V.24 module	ST2511 FlexWAN module	ST2513 Analog Conventional-to-IP Interface Kit

Functional Router Description	S2500 I/O Module Slot A Port 2	S2500 I/O Module Slot B Port 3	S2500 Analog Module Slot Ports 4, 5, 6, 7
Remote Site Router – circuit-based Conventional channels support plus Digital CCGW	ST2514 V.24 module	ST2511 FlexWAN module	Empty or ST2513 Analog Conventional-to-IP Interface Kit

*ST2510 is used for flexible site Ethernet site links. See the *Flexible Site and InterZone Links* manual.

NOTICE: While both the V.24 module (ST2514) and the Analog Conventional-to-IP Interface Kit (ST2513) may be physically present in the remote site router, only one module is operational. If the site type is configured as “digital” from the LDAP server, the V.24 module is operational. If the site type is configured as “analog” from the LDAP server, the Analog Conventional-to-IP Interface Kit (E&M module plus DSP SIMM) is operational.

7.2.2 IP Simulcast Remote Site Router – Installation and Configuration

Prerequisites: Prepare the required cabling and connectors.

Process:

1. Install the IP Simulcast remote site router in a rack. See S2500 Introduction, Installation, and Configuration on page 66.
2. Connect the IP Simulcast remote site router to a power source. See S2500 Introduction, Installation, and Configuration on page 66.
3. If necessary, ground the IP Simulcast remote site router. See S2500 Introduction, Installation, and Configuration on page 66.
4. Connect the equipment to the IP Simulcast remote site router. See IP Simulcast Remote Site Router Cabling on page 175.
5. Configure the IP Simulcast remote site router. See S2500 Introduction, Installation, and Configuration on page 66.

7.2.2.1 IP Simulcast Remote Site Router Cabling

Table 62: IP Simulcast Remote Site Router Cable Connections

From Router		To Destination Device		
Port	Connector Type	Port	Connector Type	Description
LAN 1	RJ-45	Port 1, Remote Site Switch	RJ-45	Communications connection between the router and the remote site switch.
I/O Module A	T1/E1	Remote Site Access Router WAN Link	T1/E1	Communications connection between the router and the prime site when no circuit-based Conventional channel is present.

From Router		To Destination Device		
Port	**Connector Type**	**Port**	**Connector Type**	**Description**
	or Ethernet 10Base-T (if using Flexible Ethernet Site Links)	Remote Site Access Router WAN Link	RJ-45	Communications connections between the router and the prime site when flexible site links are used.
	or V.24 (RJ-45)	Modem or base station	RJ-45-to-25 "D" adapter or RJ-45	Use these connections when the remote site router is used as a digital CCGW.
I/O Module B	FlexWAN	Channel Bank (remote site)	FlexWAN	Use these connections when a circuit-based Conventional channel is present.
	or V.24 (RJ-45)	Modem or base station	RJ-45-to-25 “D” adapter or RJ-45	Use these connections when the remote site router is used as a digital CCGW.
Analog Module	Conventional-to-IP Interface Kit	E&M relay interfaces to analog conventional base stations	Conventional-to-IP Interface Kit	Use these connections when the remote site router is used as an analog CCGW.
Console	RS232/DB9	Console/Terminal, Serial Port	RS232/DB9	Communications connection between the router and a console or terminal.

7.2.3 IP Simulcast Remote Site Router – Maintenance and Troubleshooting

Generic maintenance and troubleshooting procedures apply. For maintenance and troubleshooting information, refer to S2500 Introduction, Installation, and Configuration on page 66.

7.3 IP Simulcast Subsystem Remote Site Access Router

The IP Simulcast Remote Site Access Router is the interface between the prime site router and the remote site router.

7.3.1 IP Simulcast Remote Site Access Router – Functional Description

The IP Simulcast Remote Site Access Router is the interface between the prime site router and the remote site router. The remote site access router interfaces to the prime site router through its Ethernet LAN port and connects to the remote site router through a WAN Link. The remote site access router requires the 12-port T1/E1 module when deployed in a Cooperative WAN Routing (CWR) arrangement.

NOTICE: If the remote site access routers are configured for encryption, see the *Link Encryption and Authentication* manual for details about installation and configuration issues specific to router encryption.

7.3.1.1 Remote Site Access – Function

The remote site access routers located at the prime site, provide the IP network routing interfaces between the prime site and all of the remote site.

Depending on the remote site link configuration, remote site access can serve different functions:

Single remote link configuration
Two routers are deployed in a CWR routing arrangement.

Dual remote site link configuration
Routers serve as the endpoints for each of the remote site links.

7.3.1.2 Remote Site Access Router Overview

The Remote Site Access Router located at the IP Simulcast Prime Site provides the IP network routing interface between the prime site and the remote site. The following table lists the port connections for the Remote Site Access Routers in Prime Sites configured with 15 subsites or less.

Table 63: Port Connections for a Maximum of 15 Subsites (Standard Configuration Prime Site)

Port	Destination
	Remote Site Access Router 1
LAN 1	Prime Site Switch 1
LAN 2	Crossover to the Remote Site Access Router 2
T1/E1	Relay Panel to Remote Site
	Remote Site Access Router 2
LAN 1	Prime Site Switch 2
LAN 2	Crossover to the Remote Site Access Router 1
T1/E1	Relay Panel to Remote Site

Table 64: Port Connections for a Maximum of 15 Subsites (Geographically Redundant Prime Sites)

Port	Destination
	Remote Site Access Router 1
LAN 1	Prime Site Switch 1
LAN 3	Backhaul Switch 1
	Remote Site Access Router 2
LAN 1	Prime Site Switch 2
LAN 3	Backhaul Switch 2

A standard configuration prime site with a 32 subsite capacity is the same as a standard configuration prime site with a 15 subsite capacity, except there are three Ethernet LAN switches at the prime site. Switches #1 and #2 are paired between two subsite access routers or gateway pairs and switch #3 is connected to both subsite access router or gateway pairs (crossover cable is not utilized).

For prime sites equipped for 32 subsite capacity, the total number of CWR patch panels required is greater. The total number of CWR patch panels required depends on the site link configuration for the Simulcast subsystem.

- Single site links – two CWR patch panel
- Dual/single link combinations – three or four CWR patch panels
- Dual site links – four CWR patch panels

When using Ethernet links, each subsite access router or gateway is connected to a backhaul switch.

For more information regarding the IP Simulcast Prime Site, see the *Trunked IP Simulcast Subsystem Prime Site* manual.

Table 65: Port Connections for a Subsite Capacity Greater than 15 (Standard Configuration Prime Site)

Port	Destination
	Remote Site Access Router 1
LAN 1	Prime Site Switch 1
LAN 2	Prime Site Switch 3
T1/E1	Relay Panel to Remote Site
	Remote Site Access Router 2
LAN 1	Prime Site Switch 2
LAN 2	Prime Site Switch 3
T1/E1	Relay Panel to Remote Site
	Remote Site Access Router 3
LAN 1	Prime Site Switch 1
LAN 2	Prime Site Switch 3
T1/E1	Relay Panel to Remote Site
	Remote Site Access Router 4
LAN 1	Prime Site Switch 2
LAN 2	Prime Site Switch 3
T1/E1	Relay Panel to Remote Site

Table 66: Port Connections for a Subsite Capacity Greater than 15 (Geographically Redundant Prime Sites)

Port	Destination
	Remote Site Access Router 1
LAN 1	Prime Site Switch 1
LAN 3	Backhaul Switch 1
	Remote Site Access Router 2

Port	Destination
LAN 1	Prime Site Switch 2
LAN 3	Backhaul Switch 2
	Remote Site Access Router 3
LAN 1	Prime Site Switch 1
LAN 3	Backhaul Switch 1
	Remote Site Access Router 4
LAN 1	Prime Site Switch 2
LAN 3	Backhaul Switch 2

See Field Replaceable Units – S6000 on page 62 for a list of the I/O modules that are used to meet the functional requirements of each router.

7.3.1.3 Redundant Remote Site Links

With IP simulcast, dual site links for the remote sites are required. The CWR feature accommodates redundant remote site links through bypassing the relay function of the relay panel. An additional relay panel can also be added if needed.

The simulcast site supports a mixture of single and dual remote site links, but a 12 T1/E1 card on a remote site access router can only support one or the other type (either single site links or dual site links). The individual T1/E1s within the 12-port module cannot be wired individually.

7.3.2 IP Simulcast Remote Site Access Router – Installation and Configuration

Prerequisites: Prepare the required cabling and connectors.

Process:

1. Install the IP Simulcast Remote Site Access Router in a rack. See S6000 Introduction, Installation, and Configuration on page 27.
2. Connect the IP Simulcast Remote Site Access Router to a power source. See S6000 Introduction, Installation, and Configuration on page 27.
3. If necessary, ground the IP Simulcast Remote Site Access Router. See S6000 Introduction, Installation, and Configuration on page 27.
4. Connect the equipment to the IP Simulcast Remote Site Access Router. See Connecting the Routers to the Relay Panel (Single Site Link Configuration) on page 181, Connecting the Routers to the Relay Panel (Dual Site Link Configuration) on page 182, and Connecting the Routers to the Relay Panel (Mix Site Link Configuration) on page 183.

   NOTICE: If a Geographically Redundant Prime Site configuration is present in the system, use an Ethernet connection to the Remote Site Access Router.

5. Configure the IP Simulcast Remote Site Access Router. See S6000 Introduction, Installation, and Configuration on page 27.

7.3.2.1 Single Site Link Configuration for the Remote Site Access Router

Table 67: Port Connections for a Single Site Link Configuration

Port	Destination
Remote Site Access Router 1	
LAN 1	Prime Site Switch 1
LAN 2	Prime Site Switch 3
T1/E1	Relay Panel to Remote Site
Remote Site Access Router 2	
LAN 1	Prime Site Switch 2
LAN 2	Prime Site Switch 3
T1/E1	Relay Panel to Remote Site
Remote Site Access Router 3	
LAN 1	Prime Site Switch 1
LAN 2	Prime Site Switch 3
T1/E1	Relay Panel to Remote Site
Remote Site Access Router 4	
LAN 1	Prime Site Switch 2
LAN 2	Prime Site Switch 3
T1/E1	Relay Panel to Remote Site

Table 68: Port Connections for a Single Site Link Configuration (Geographically Redundant Prime Sites)

Port	Destination
Remote Site Access Router 1	
LAN 1	Prime Site Switch 1
LAN 3	Backhaul Switch 1
Remote Site Access Router 2	
LAN 1	Prime Site Switch 2
LAN 3	Backhaul Switch 2
Remote Site Access Router 3	
LAN 1	Prime Site Switch 1
LAN 3	Backhaul Switch 1
Remote Site Access Router 4	
LAN 1	Prime Site Switch 2
LAN 3	Backhaul Switch 2

7.3.2.2
Dual Site Link Configuration for the Remote Site Access Router

Table 69: Port Connections for a Dual Site Link Configuration

Port	Destination
Remote Site Access Router 1	
LAN 1	Prime Site Switch 1
LAN 2	Prime Site Switch 3
Module A, T1/E1	Relay Panel to Remote Site
Module B, T1/E1	1 Relay Panel to Remote Site
Remote Site Access Router 2	
LAN 1	Prime Site Switch 2
LAN 2	Prime Site Switch 3
Module A, T1/E1	Relay Panel to Remote Site
Module B, T1/E1	1 Relay Panel to Remote Site
Remote Site Access Router 3	
LAN 1	Prime Site Switch 1
LAN 2	Prime Site Switch 3
Module A, T1/E1	Relay Panel to Remote Site
Module B, T1/E1	1 Relay Panel to Remote Site
Remote Site Access Router 4	
LAN 1	Prime Site Switch 2
LAN 2	Prime Site Switch 3
Module A, T1/E1	Relay Panel to Remote Site
Module B, T1/E1	1 Relay Panel to Remote Site

For port connections for a dual site link configuration in Geographically Redundant Prime Sites, see Table 68: Port Connections for a Single Site Link Configuration (Geographically Redundant Prime Sites) on page 180.

7.3.2.3
Connecting the Routers to the Relay Panel (Single Site Link Configuration)

Prerequisites: Prepare

- If your application requires 12 or fewer T1/E1 ports, two 12-port relay cables
- If your application requires 13-24 T1/E1 ports, four 2-port relay cables

When and where to use: Perform this procedure to properly connect the 12-port T1/E1 modules of the router to the relay panel through 12-port relay cables.

NOTICE: This procedure does not apply to Geographically Redundant Prime Sites.

Procedure:

1. Connect the male end of the 12-port relay cable #1 to the 12-port T1/E1 module installed in slot A (WAN port 4) on router A.
2. Connect the female end of the 12-port relay cable #1 to the upper-left WAN connector (labeled Router A WAN Module 1) on the relay panel.
3. Connect the male end of the 12-port relay cable #2 to the 12-port T1/E1 module installed in slot A (WAN port 4) on router B.
4. Connect the female end of the 12-port relay cable #2 to the upper-right WAN connector (labeled Router B WAN Module 1) on the relay panel.
5. Do one of the following:
   - If your application requires 12 or fewer T1/E1 ports, proceed to step 10.
   - If your application requires 13-24 T1/E1 ports, proceed to step 6.
6. Connect the male end of the 12-port relay cable #3 to the 12-port T1/E1 module installed in slot B (WAN port 5) on router A.
7. Connect the female end of the 12-port relay cable #3 to the lower-left WAN connector (labeled Router A WAN Module 2) on the relay panel.
8. Connect the male end of the 12-port relay cable #4 to the 12-port T1/E1 module installed in slot B (WAN port 5) on router B.
9. Connect the female end of the 12-port relay cable #4 to the lower-right WAN connector (labeled Router B WAN Module 2) on the relay panel.
10. Connect the T1/E1 ports on the right of the relay panel to the appropriate T1/E1 ports on the device on the other side of the site or InterZone link.

7.3.2.4

Connecting the Routers to the Relay Panel (Dual Site Link Configuration)

This section explains how to connect the routers to the relay panel for a dual site link configuration using 24 dual site links.

Prerequisites: Ensure you have four 12-port relay cables prepared.

When and where to use: Perform the following procedure to properly connect the 12-port T1/E1 modules of the router to the relay panel through 12-port relay cables.

NOTICE: This procedure does not apply to Geographically Redundant Prime Sites.

Procedure:

1. Connect the male end of 12-port relay cable #1 to the 12-port T1/E1 module installed in slot A (WAN port 4) on router A.
2. Connect the female end of 12-port relay cable #1 to the upper-left WAN connector (labeled Router A WAN Module 1) on relay panel #1.
3. Connect the male end of 12-port relay cable #2 to the 12-port T1/E1 module installed in slot B (WAN port 5) on router A.
4. Connect the female end of 12-port relay cable #2 to the lower-left WAN connector (labeled Router A WAN Module 2) on relay panel #1.

5. Connect the male end of 12-port relay cable #3 to the 12-port T1/E1 module installed in slot A (WAN port 4) on router B.
6. Connect the female end of 12-port relay cable #3 to the upper-right WAN connector (labeled Router B WAN Module 1) on relay panel #2.
7. Connect the male end of 12-port relay cable #4 to the 12-port T1/E1 module installed in slot B (WAN port 5) on router B.
8. Connect the female end of 12-port relay cable #4 to the lower-right WAN connector (labeled Router B WAN Module 2) on relay panel #2.

7.3.2.5 Connecting the Routers to the Relay Panel (Mix Site Link Configuration)

This section describes how to connect the routers to the relay panel for a mix site link configuration using 12 single links and 12 dual links.

Prerequisites: Ensure you have four 12-port relay cables prepared.

When and where to use: Perform the following procedure to properly connect the 12-port T1/E1 modules of the router to the relay panel through 12-port relay cables.

NOTICE: This procedure does not apply to Geographically Redundant Prime Sites.

Procedure:

1. Connect the male end of 12-port relay cable #1 to the 12-port T1/E1 module installed in slot A (WAN port 4) on router A.
2. Connect the female end of 12-port relay cable #1 to the upper-left WAN connector (labeled Router A WAN Module 1) on relay panel #1.
3. Connect the male end of 12-port relay cable #2 to the 12-port T1/E1 module installed in slot B (WAN port 5) on router A.
4. Connect the female end of 12-port relay cable #2 to the lower-left WAN connector (labeled Router A WAN Module 2) on relay panel #1.
5. Connect the male end of 12-port relay cable #3 to the 12-port T1/E1 module installed in slot A (WAN port 4) on router B.
6. Connect the female end of 12-port relay cable #3 to the lower-right WAN connector (labeled Router A WAN Module 2) on relay panel #1.
7. Connect the male end of 12-port relay cable #4 to the 12-port T1/E1 module installed in slot B (WAN port 5) on router B.
8. Connect the female end of 12-port relay cable #4 to the lower-right WAN connector (labeled Router B WAN Module 2) on relay panel #2.

7.3.3 IP Simulcast Remote Site Access Router – Maintenance and Troubleshooting

For maintenance and troubleshooting information, refer to S6000 Introduction, Installation, and Configuration on page 27. Generic maintenance and troubleshooting procedures apply.

7.3.3.1 Relay Panel Failure

The relays are latching and retain their last state during power failures, or loss of communications with the core and exit routers. There is no loss of connectivity.

7.3.3.2 Remote Site Access Router Failure

An S6000 Router may contain up to 24 T1/E1 ports. The routers are deployed in pairs as Active and Inactive. The router failures are as follows:

- The connection between the Active router and the relay panel fails. This is detected by the router hardware. Once it is detected, a signal is sent to the relay to switch all associated ports to the Inactive router.
- Individual site or InterZone links fail. These failures do not cause switching between the routers.
- The Active router fails completely. This is detected by the Inactive router through the communication between the two routers. Once the failure is detected, the Inactive router switches all the relays to itself, and becomes the Active router.
- In the event of a total damage of the relay panel, it is possible to lose all of the sites connected to the panel. However, power failures and communication failures to the panel leave all the site links connected to one of the routers.

7.3.3.3 Cooperative WAN Routing Troubleshooting Tools

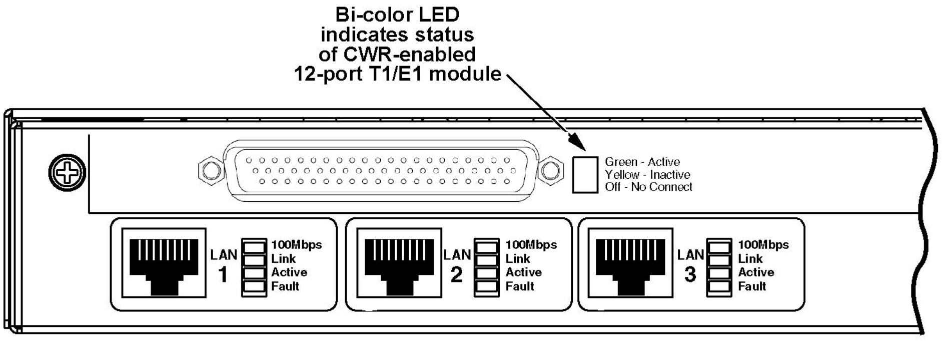
The tools used for troubleshooting CWR are as follows:

- Unified Event Manager
- Unified Network Configurator
- InfoVista
- Local Router Administration

7.3.3.4 12-Port T1/E1 (CWR) Module LED

The 12-port T1/E1 module features a single bi-color LED. The LED indicates CWR status of the module.

Figure 53: 12-Port T1/E1 (CWR) Module LED



CWR_12port_T1E1_module_LED

Table 70: 12-Port T1/E1 (CWR) Module LED

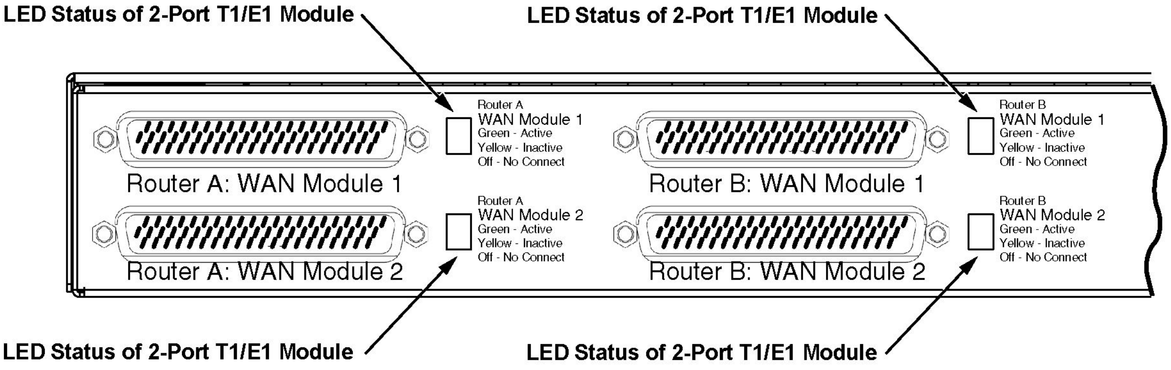
LED	Indication	Status and Troubleshooting Action
Bi-color LED	Green	The module is connected to the relay panel and is functioning as the active CWR peer.
	Amber	The module is connected to the relay panel and is functioning as the inactive CWR peer.
	OFF	The module is not connected to the relay panel.

7.3.3.5

Relay Panel LEDs

The relay panel features four bi-color LEDs, one for each 12-port T1/E1 module to relay panel connection. Each LED on the relay panel corresponds to a WAN connector, and indicates CWR status of the 12-port T1/E1 module connected to that connector.

Figure 54: Relay Panel LEDs



CWR_Relay_panel_LEDs

Table 71: Relay Panel LEDs

LED	Indication	Status and Troubleshooting Action
Router A WAN module 1 LED, or Router A WAN module 2 LED, or Router B WAN module 1 LED, or Router B WAN module 2 LED.	Green	The module is connected to the relay panel, and is functioning as the active CWR peer.
	Amber	The module is connected to the relay panel, and is functioning as the inactive CWR peer.
	OFF	The module is not connected to the relay panel.

Chapter 8

ASTRO 25 Trunking Subsystem

This chapter provides information about the S6000 Router in an ASTRO® 25 trunking subsystem.

The S6000 Router in an ASTRO® 25 trunking subsystem prime site provides the following router functions:

- Prime Site Router
- Remote Site Access Router

The ASTRO® 25 trunking subsystem supports ASTRO 25® repeater sites and/or simulcast/voting subsystems, dispatch sites, and centralized conventional sites for trunking and conventional channel operation. The S6000 Router is available as a Conventional Channel Gateway (CCGW) interface device in a variety of different hardware configurations to support various types of conventional channels in your system. See CCGW Interfaces on page 215.

8.1 Trunking Subsystem Prime Site Router

The trunking subsystem prime site router handles the traffic between the prime site network and the zone core.

8.1.1 Trunking Subsystem Prime Site Router – Functional Description

The S6000 prime site router handles the traffic between the prime site network and the zone core.

The prime site router distributes voice, control, and network management traffic to the appropriate devices on the prime site network.

NOTICE: For additional information on the trunking subsystem prime site as a whole, see the *Edge Availability with Wireline Console Feature Guide for Trunking Subsystems* manual. If the prime site routers are configured for encryption, see the *Link Encryption and Authentication* manual for details about installation and configuration issues specific to router encryption.

8.1.1.1 Trunking Subsystem Prime Site Router – Function

The prime site router directs all control, voice, and network management traffic between the prime site LAN and the site link to the zone core using an Ethernet WAN Backhaul link. The router connects the Ethernet LAN through a LAN port. An optional redundant prime site router can be installed in the prime site.

The site can be set up to benefit from the zone core redundancy afforded by Dynamic System Resilience (DSR), or designed to connect to one zone core only as in systems without DSR. For detailed information on a DSR configuration, see the *Dynamic System Resilience Feature Guide* manual.

If a Geographically Redundant Prime Site configuration is present in the system, two prime site routers are required: the Primary and Secondary Prime Site Router.

The prime site routers functions are:

Media conversion

The router converts the 100 MB Ethernet LAN packets to IP packets encapsulated in Frame Relay on a serial WAN interface or to tunneled IP packets on an Ethernet flexible site link.

Traffic prioritizing

The router applies the correct prioritization masking to the packets leaving the site.

Fragmentation

The router fragments large IP packets per standards.

Dynamic Host Configuration Protocol (DHCP) service

This service allows the technician to connect to the LAN at the site using a properly configured PC with the Windows OS.

The prime site router is based on the Motorola Network Router (MNR) S6000. Three built-in Ethernet ports (LAN ports) provide connectivity to the site Ethernet switch, where Tsub zone controller is accessible.

The prime site router facilitates network management activity at the site and provides a medium for receiving and reporting failure alarms. The Unified Network Configurator (UNC), Unified Event Manager (UEM), and MOSCAD Network Fault Management (NFM) have access to the prime site and any connected remote subsites through the prime site router and remote site access router.

8.1.1.2 Trunking Subsystem Prime Site Router to Zone Core Links

A link is defined as both the physical and logical connections between two entities. The link type used in a prime site to zone core connection is called a site link.

Table 72: Prime Site to Zone Core Site Link Type

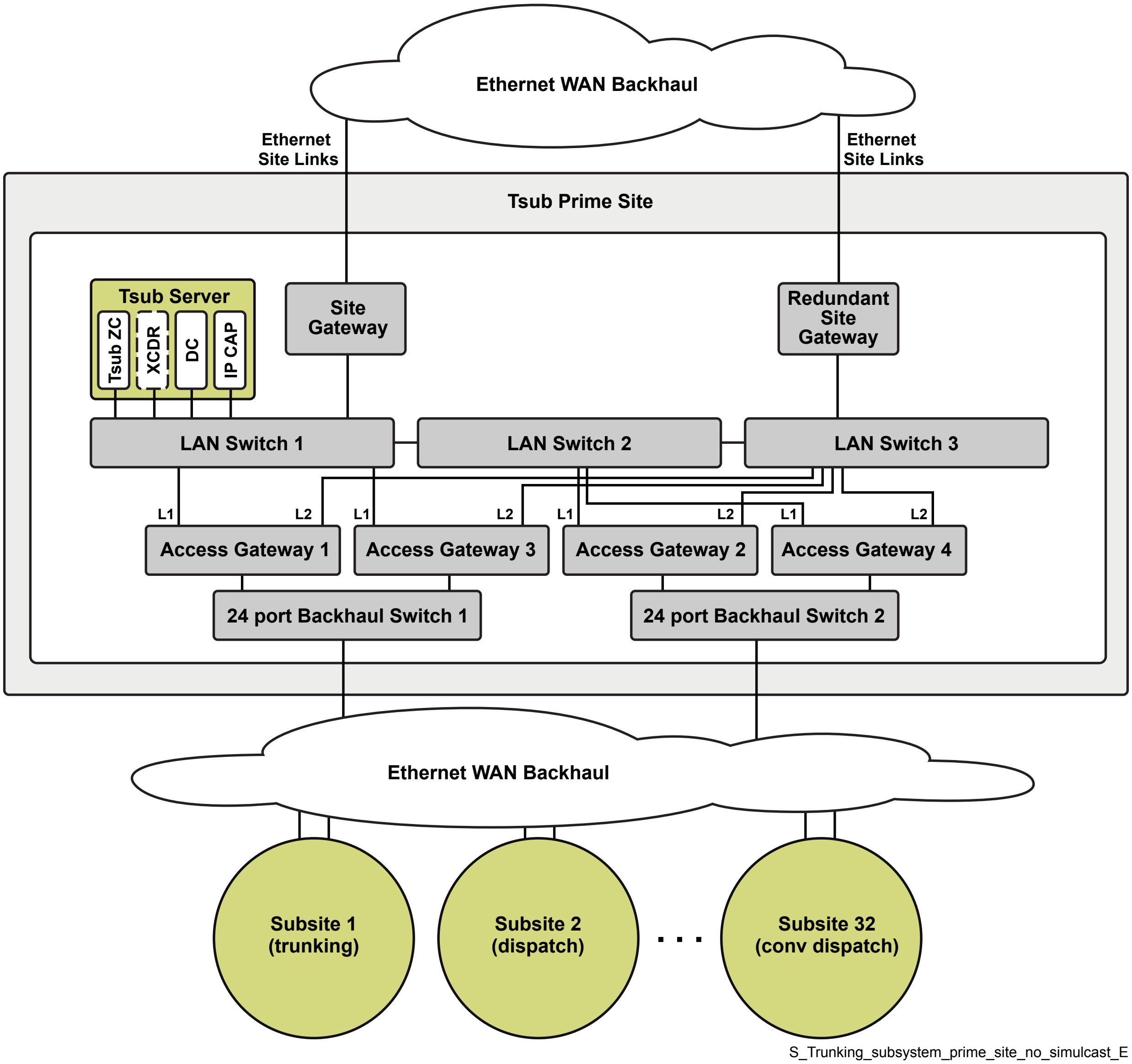
Link Name	Physical Description	Logical Description
Site Link	Connects the zone core and prime site using an Ethernet connection between the WAN backhaul switch at the zone core and prime site router.	Provides the physical connection between the redundant core routers at the zone core and prime site router. The physical connection is used to set up the logical links. Logical path is from the prime site router to the WAN backhaul switch at the zone core.

The trunking subsystem allows for a single site link and dual site links between prime and zone cores.

Figure 55: Trunking Subsystem Single or Dual Site Links Prime Site on page 188 shows a representative prime site configuration with a single and a redundant prime site router link (optional) going to the zone core.

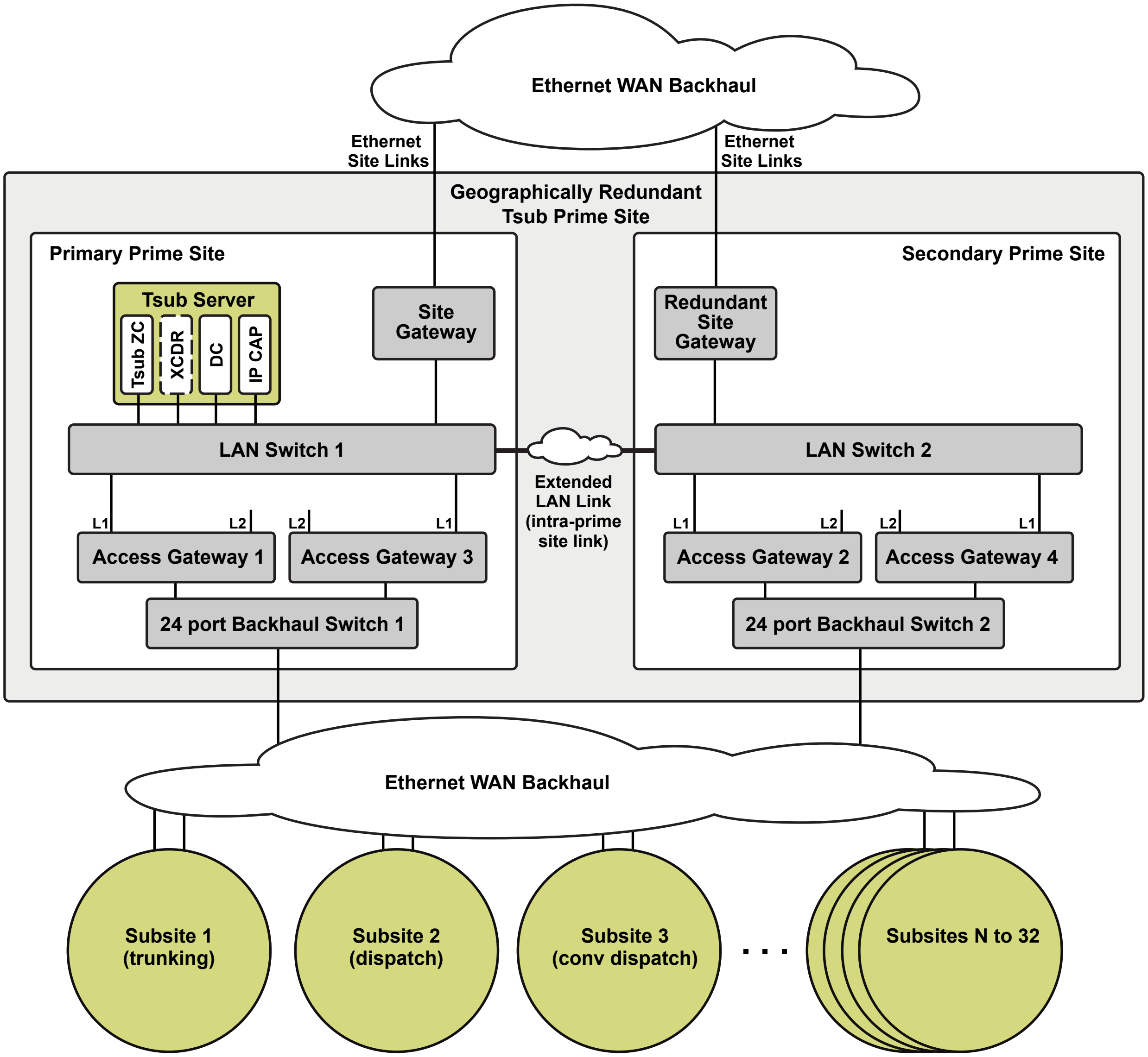
NOTICE: Single site links between the prime site and zone core do not apply to systems with the Geographically Redundant Prime Site configuration. Dual site links are present in those systems. See Figure 56: Trunking Subsystem Dual Site Links of a Geographically Redundant Prime Site on page 189.

Figure 55: Trunking Subsystem Single or Dual Site Links Prime Site



NOTICE: The redundant prime site router (optional) in the diagram, is not included in a single router link configuration to the zone core.

Figure 56: Trunking Subsystem Dual Site Links of a Geographically Redundant Prime Site



S_Trunking_subsystem_redundancy_no_simulcast_E

NOTICE: If Dynamic System Resilience is implemented on your system, see the *Dynamic System Resilience* manual for details on connections and diagrams relating to the prime site router.

8.1.1.3
Trunking Subsystem Prime Site Router Connections

The prime site router has an Ethernet connection to the zone core and an Ethernet connection to the prime site LAN switch.

Audio and control traffic is processed by the zone controllers in the zone core or by the Tsub zone controller at the prime site if connectivity to the zone controllers in the zone core is lost. The prime site router distributes audio and control traffic to the prime site LAN.

The audio and control traffic intended for the zone core is sent to the prime site router over the prime site LAN. The prime site router delivers the traffic over the Ethernet link to the zone core.

The prime site can be set up to benefit from the zone core redundancy afforded by Dynamic System Resilience (DSR), or designed to connect to one zone core only as in systems without DSR.

- If the prime site is set up not to use DSR, the connections are made from the site router(s) to one zone core only.
- If the prime site is set up to use DSR, the connections are made to both primary and backup zone cores.

NOTICE: Contact your system administrator or refer to your customized system configuration plan for prime site router port connections in a DSR scenario. For detailed information on a Dynamic System Resilience configuration, see the *Dynamic System Resilience Feature Guide* manual.

If the Geographically Redundant Prime Site configuration is present in the system, two prime site routers are required: the Primary and Secondary Prime Site Router.

Table 73: Port Connections for the Prime Site Routers

Port	Destination
Prime Site Router 1	
LAN 1	Prime Site Switch 1
LAN 3	Ethernet WAN link to the zone core
Prime Site Router 2	
LAN 1	Prime Site Switch 2
LAN 3	Ethernet WAN link to the zone core

8.1.1.4

Trunking Subsystem Prime Site Router – EOS Functions

A certain list of interfaces, protocols, basic routing, and IP features in the Enterprise OS (EOS) is used by the prime site router.

The prime site router uses basic routing and IP features in the Enterprise OS (EOS) software including the following:

- IP Routing
- 10/100 Ethernet
- Static Routes
- Fragmentation
- Flexible Ethernet Links

The prime site router uses the following protocols and interfaces:

- Simple Network Management Protocol (SNMP)
- Multicast
- Type of Service (TOS)
- Dynamic Host Configuration Protocol (DHCP)
- Network Time Protocol (NTP)

8.1.2 Trunking Subsystem Prime Site Router - Installation and Configuration

Prerequisites: Prepare the required cabling and connectors.

Procedure:

1. Install the prime site router in a rack. See S6000 Introduction, Installation, and Configuration on page 27.
2. Connect the prime site router to a power source. See S6000 Introduction, Installation, and Configuration on page 27.
3. If necessary, ground the prime site router. See S6000 Introduction, Installation, and Configuration on page 27.
4. Connect the equipment to the prime site router. See Trunking Subsystem Prime Site Router Cabling on page 191.
5. Configure the prime site router. See S6000 Introduction, Installation, and Configuration on page 27.

8.1.2.1 Trunking Subsystem Prime Site Router Cabling

This section describes how to cable each interface on the prime site routers.

NOTICE: If a Dynamic System Resilience (DSR) configuration is implemented on your system, see Trunking Subsystem Prime Site Router Connections on page 189 for details.

Table 74: Cable Connections from the Prime Site Router

From Prime Site Router		Destination Device		
Port	**Connector Type**	**Port**	**Connector Type**	**Description**
LAN 1	RJ45	Port 1, Prime Site Switch 1	RJ45	Connection to the prime site switch
LAN 3	Ethernet 10Base-T	Zone core WAN Link	RJ45	Ethernet connection to the zone core

NOTICE: If a redundant router is used, connect LAN 1 to the corresponding ports on Switch 2.

8.1.2.2 Router Encryption Card Installation and Configuration

For more information, see the *Link Encryption and Authentication* manual.

8.1.3

Trunking Subsystem Prime Site Router - Maintenenace and Troubleshooting

Generic maintenance and troubleshooting procedures apply. For maintenance and troubleshooting information, see S6000 Introduction, Installation, and Configuration on page 27.

8.1.3.1

Router Encryption Card Troubleshooting

See the *Link Encryption and Authentication* manual for more information.

8.2

Trunking Subsystem Remote Site Access Router

The trunking subsystem remote site access router is the interface between the prime site router and the remote site router.

8.2.1

Trunking Subsystem Remote Site Access Router – Functional Description

The trunked subsystem remote site access router is the interface between the prime site router and a site router located at a remote subsite using Ethernet links. The remote site access router interfaces to the prime site router through its Ethernet LAN port. The remote site access router interfaces to a remote subsite router through a backhaul switch that connects through an Ethernet WAN Backhaul link.

NOTICE: If the remote site access routers are configured for encryption, see the *Link Encryption and Authentication* manual for details about installation and configuration issues specific to router encryption.

8.2.1.1

Trunking Subsystem Remote Site Access Router Function

The remote site access routers located at the prime site, provide the IP network routing interfaces between the prime site and all of the remote subsites.

Depending on the remote site link configuration, a remote site access router can serve different functions:

Single remote link configuration
Two routers (1 pair) are deployed, each having a logical link established to a single subsite router.

Dual remote site link configuration
Routers serve as the endpoints for each of the remote site links.

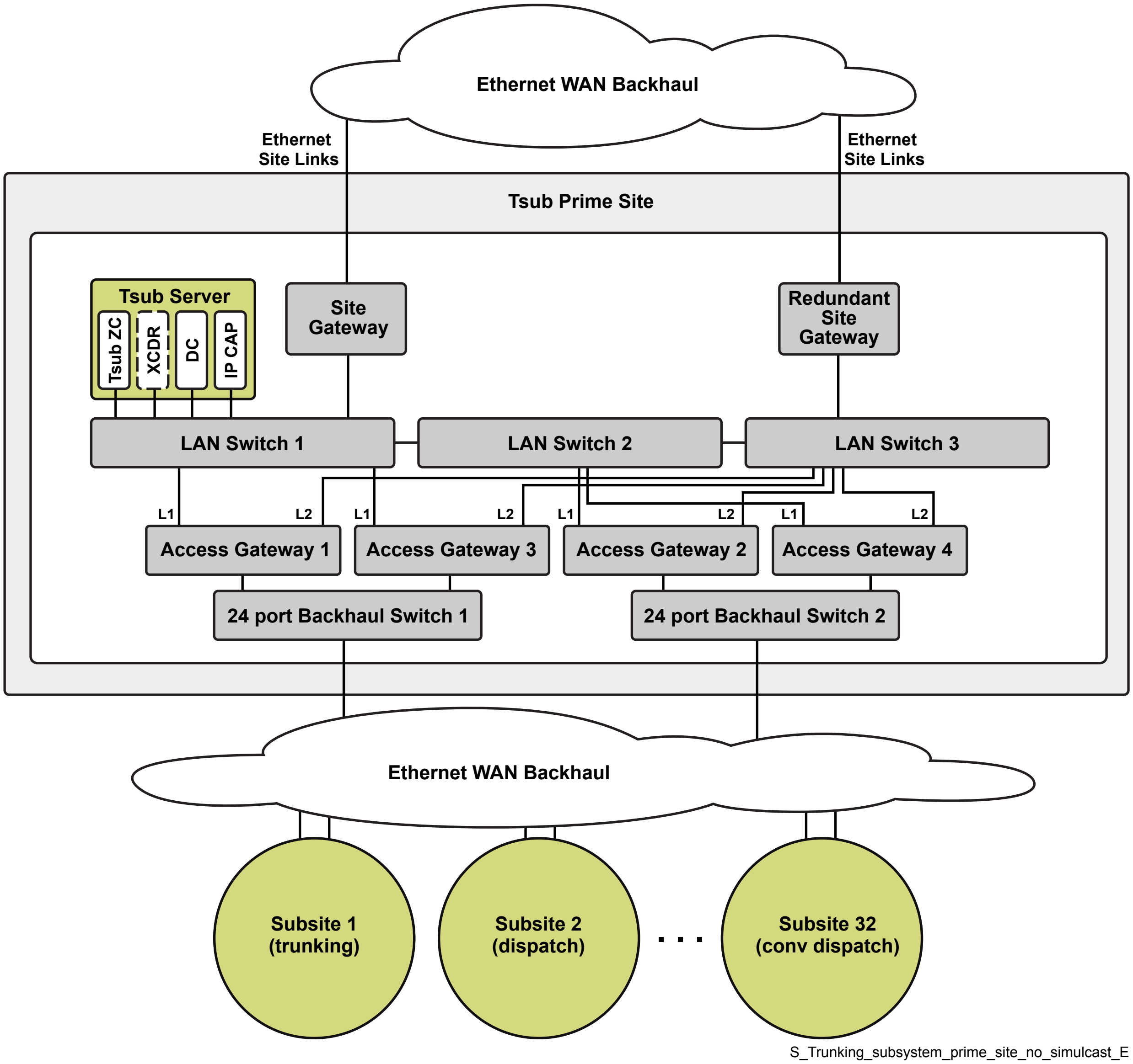
Gateway function
A remote site access router serves as the gateway if both prime site routers fail.

8.2.1.2

Trunking Subsystem Redundant Remote Site Access Links

With a trunking subsystem, dual site links to the remote subsites are highly recommended. The trunking subsystem supports a mixture of single and dual remote site links.

Figure 57: Trunking Subsystem Dual Site Links to the Remote Subsites



8.2.2

Trunking Subsystem Remote Site Access Router - Installation and Configuration

Prerequisites: Prepare the required cabling and connectors.

Procedure:

1. Install the remote site access router in a rack. See S6000 Introduction, Installation, and Configuration on page 27.
2. Connect the remote site access router to a power source. See S6000 Introduction, Installation, and Configuration on page 27.
3. If necessary, ground the remote site access router. See S6000 Introduction, Installation, and Configuration on page 27.

4 Connect the switches and backhaul switch to the remote site access router.

5 Configure the remote site access router. See S6000 Introduction, Installation, and Configuration on page 27.

8.2.2.1
Port Connections for a Maximum of 15 Subsites

The following table lists the port connections for the remote site access routers in prime sites configured with 15 subsites or less.

Table 75: Port Connections for a Maximum of 15 Subsites (Standard Configuration Prime Site)

Port	Destination
Remote Site Access Router 1	
LAN 1	Prime Site Switch 1
LAN 2	Crossover to the Remote Site Access Router 2
LAN 3	Backhaul Switch 1
Remote Site Access Router 2	
LAN 1	Prime Site Switch 2
LAN 2	Crossover to the Remote Site Access Router 1
LAN 3	Backhaul Switch 2

Table 76: Port Connections for a Maximum of 15 Subsites (Geographically Redundant Prime Sites)

Port	Destination
Remote Site Access Router 1	
LAN 1	Prime Site Switch 1
LAN 3	Backhaul Switch 1
Remote Site Access Router 2	
LAN 1	Prime Site Switch 2
LAN 3	Backhaul Switch 2

8.2.2.2
Port Connections for a Subsite Capacity Greater than 15

A standard configuration prime site with a 32 subsite capacity is the same as a standard configuration prime site with a 15 subsite capacity, except there are three Ethernet LAN switches at the prime site. Switches #1 and #2 are paired between two subsite access router pairs and switch #3 is connected to both subsite access router pairs (crossover cable is not utilized). Each subsite access router is connected to a backhaul switch.

Table 77: Port Connections for a Subsite Capacity Greater than 15 (Standard Configuration Prime Site)

Port	Destination
Remote Site Access Router 1	
LAN 1	Prime Site Switch 1

Port	Destination
LAN 2	Prime Site Switch 3
LAN 3	Backhaul Switch 1
Remote Site Access Router 2	
LAN 1	Prime Site Switch 2
LAN 2	Prime Site Switch 3
LAN 3	Backhaul Switch 2
Remote Site Access Router 3	
LAN 1	Prime Site Switch 1
LAN 2	Prime Site Switch 3
LAN 3	Backhaul Switch 1
Remote Site Access Router 4	
LAN 1	Prime Site Switch 2
LAN 2	Prime Site Switch 3
LAN 3	Backhaul Switch 2

Table 78: Port Connections for a Subsite Capacity Greater than 15 (Geographically Redundant Prime Site)

Port	Destination
Remote Site Access Router 1	
LAN 1	Prime Site Switch 1
LAN 3	Backhaul Switch 1
Remote Site Access Router 2	
LAN 1	Prime Site Switch 2
LAN 3	Backhaul Switch 2
Remote Site Access Router 3	
LAN 1	Prime Site Switch 1
LAN 3	Backhaul Switch 1
Remote Site Access Router 4	
LAN 1	Prime Site Switch 2
LAN 3	Backhaul Switch 2

8.2.3 Trunking Subsystem Remote Site Access Router - Maintenance and Troubleshooting

For maintenance and troubleshooting information, refer to S6000 Introduction, Installation, and Configuration on page 27. Generic maintenance and troubleshooting procedures apply.

8.2.3.1
Remote Site Access Router Failure

The routers are deployed in pairs as Active and Inactive. The router failures are as follows:

- The connection between the Active router and the backhaul switch fails. This is detected by the router hardware. Once it is detected,all traffic traverses the backup router. (With Ethernet links, both routers are active).
- Individual site or InterZone links fail. These failures do not cause switching between the routers.
- The Active router fails completely. This is detected by the Inactive router through the communication between the two routers. Once the failure is detected, the Inactive router switches to itself, and becomes the Active router.
- In the event of a backhaul switch failure, traffic continues through the other backhaul switch and router pair, leaving all remote site links connected. However, in the event of a backhaul switch failure and the router pair connected to the other backhaul switch failure, the remote sites enter Failsoft mode.

8.2.3.2
WAN Routing Troubleshooting Tools

The tools used for troubleshooting the WAN routing are as follows:

- Unified Event Manager
- Unified Network Configurator
- InfoVista
- Local Router Administration
- Zone Watch

Chapter 9

ASTRO 25 Conventional Master Site (K Core)

This chapter provides information on the S6000 router in an ASTRO® 25 system Small Conventional Configurations (K core). The ASTRO® 25 system Conventional Integrated Voice & Data architecture includes the K core, Conventional Hub Sites, and Conventional Base Radio Sites.

NOTICE: The GGM 8000 can be used as a replacement for the S6000 GGSN (GPRS Gateway Support Node) routers employing Ethernet site links. See the *GGM 8000 System Gateway* manual for details.

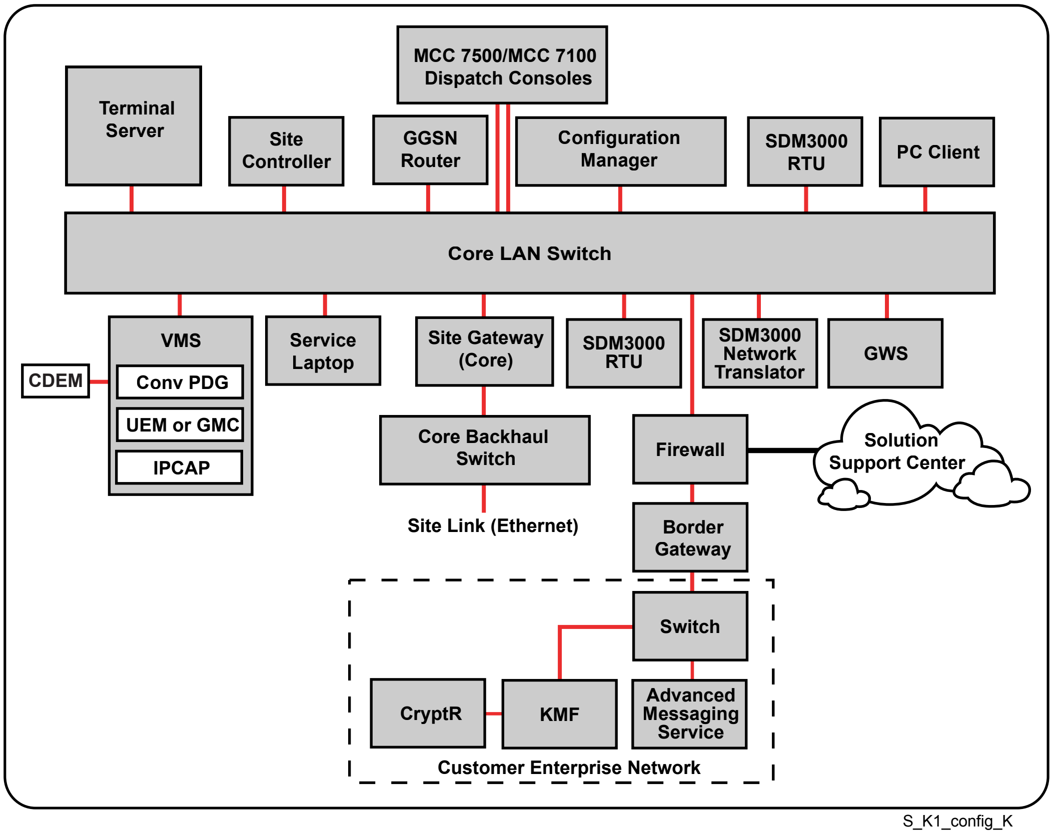
9.1 GGSN Router (K Core) – Functional Description

Motorola's implementation of GPRS Gateway Support Node (GGSN) functionality on Motorola Network Router (MNR) S6000 routers enables conventional packet data capability for mobile subscriber radios on the system.

The GGSN router at the Conventional Master Site serves as the network interface between the Motorola Solutions radio network and the Customer Enterprise Network (CEN). One side of the GGSN connects to the Motorola Solutions Radio Network Infrastructure (RNI) while the other side attaches to a peripheral network to interface with the border gateway of the CEN. The GGSN is designed to handle IP routing services for end-to-end data messaging on the ASTRO® 25 system.

The diagram below is an example to show the GGSN router connections at the Conventional master site.

Figure 58: K1 Zone Core Master Site



9.2 GGSN Router (K Core) – Installation and Configuration

Prerequisites: Ensure you have the required cabling and connectors.

Process:

1. Install the GGSN router in a rack. See S6000 Introduction, Installation, and Configuration on page 27.
2. Connect the GGSN router to a power source. See S6000 Introduction, Installation, and Configuration on page 27.
3. If necessary, ground the GGSN router. See S6000 Introduction, Installation, and Configuration on page 27.
4. Connect the equipment to the GGSN router. See GGSN Router (K Core) Cabling on page 199.
5. Configure the GGSN router. See S6000 Introduction, Installation, and Configuration on page 27.

9.2.1

GGSN Router (K Core) Cabling

The GGSN router has three Ethernet ports using RJ-45 connectors. Two of the Ethernet ports connect to the Ethernet LAN switch, and the console port connects to the terminal server. The following table describes these connections.

Table 79: GGSN Router at Conventional Master Site Cable Connections

From GGSN Port	Connector Type	To Destination Device	Port	Notes
LAN 1/LAN 2	RJ-45	Master Site Ethernet LAN Switch	See Notes column	Refer to the customized port configuration information provided by Motorola Solutions for your system master site.
Console	DB-9	Optional Console/ Terminal server connection	Serial	Terminal server connects for remote service access to GGSN.

9.3

GGSN Router (K Core) – Maintenance and Troubleshooting

If there is a failure on the GPRS Gateway Support Node (GGSN) router, the system loses the ability to provide data messaging from your data network to mobile data devices in your system and all IP services are dropped. If the GGSN router has issues, fault information is retrieved from the local logs from a service PC. If the router is not accessible from the service PC, then no fault information is available.

Chapter 10

ASTRO 25 Customer Enterprise Network

This chapter provides information on the routers in the Customer Enterprise Network (CEN).

10.1 Border Router

This section contains information specific to the S6000 when used as a Border Router.

10.1.1 Border Router – Functional Description

The border router serves as the demarcation between a peripheral network and the Motorola Solutions Radio Network Infrastructure (RNI). The border router demarcates the point where Motorola responsibilities end and your organization's begin. The border router connects the De-Militarized Zone (DMZ) to the Customer Enterprise Network (CEN) and uses a Dynamic Host Configuration Protocol (DHCP). The border router may be customer supplied, and could be a firewall. The border routers are required for all connections to a CEN.

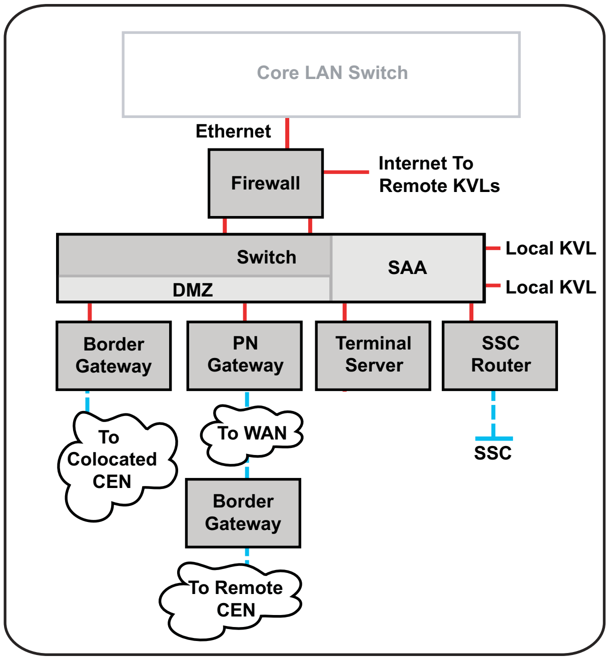
The border router can be either a S6000 router or GGM 8000 Gateway.

If a CEN is geographically separated from the RNI, the border router backhaul LAN/WAN connection is terminated on a peripheral network router that is colocated with the RNI. The peripheral network router terminates at the De-Militarized Zone (DMZ) provided by the RNI-DMZ firewall.

If a CEN is geographically colocated with the RNI, the border router backhaul LAN connection is directly terminated at the DMZ provided by the RNI-DMZ firewall. No peripheral network router is required for this scenario.

The border routers can also be used to provide connectivity between unique CENs by the use of IPIP tunnels.

Figure 59: Border Router – System Context

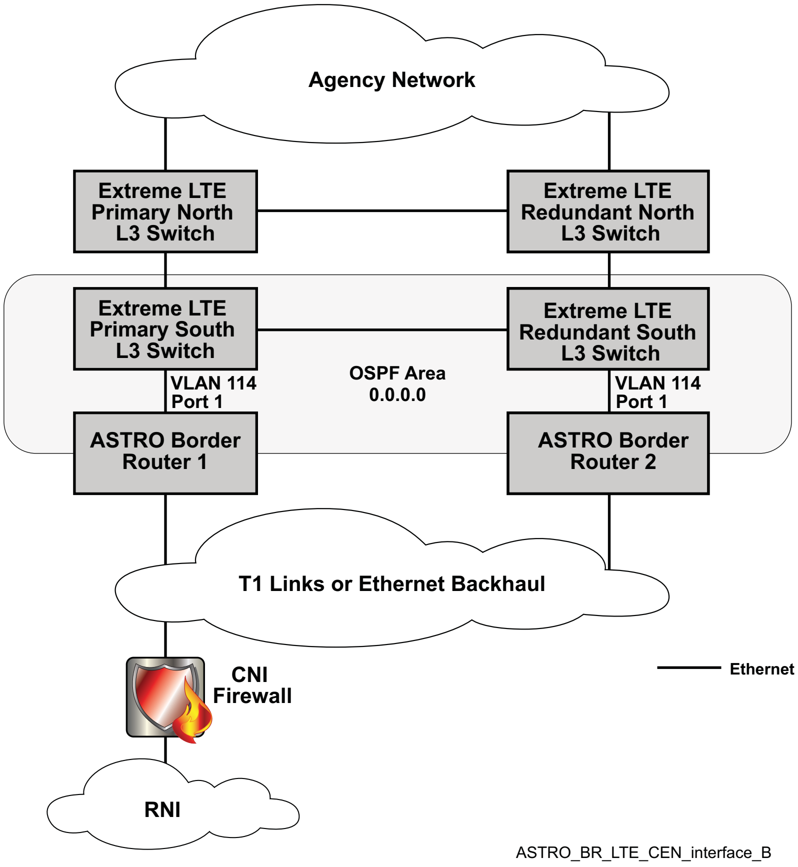


S_Firewall_Option_With_Switch_B

NOTICE: If Dynamic System Resilience is implemented on your system, a minimum of two border routers associated with the same DSR Master Site pair must terminate at the same CEN. Refer to the *Dynamic System Resilience Feature Guide* manual for details on connections and diagrams relating to the border router.

In the ASTRO/LTE CEN configuration, if present in the system, the ASTRO Border Router(s) interface to LTE switching and routing equipment. Both single and dual Border Router configurations are supported. In case of dual Border Router configuration, one VLAN is provided on both Border Router connections. The OSPF protocol is used between the Border Router(s) and the LTE Primary South Router and Primary North Router.

Figure 60: ASTRO/LTE CEN Interface


Agency Network
Extreme LTE Primary North L3 Switch
Extreme LTE Redundant North L3 Switch
Extreme LTE Primary South L3 Switch
Extreme LTE Redundant South L3 Switch
OSPF Area 0.0.0.0
VLAN 114 Port 1
VLAN 114 Port 1
ASTRO Border Router 1
ASTRO Border Router 2
T1 Links or Ethernet Backhaul
CNI Firewall
Ethernet
RNI
ASTRO_BR_LTE_CEN_interface_B

10.1.1.1
Border Routers – EOS Functions

The border router uses basic routing and IP features in the Enterprise OS (EOS) software.

Functions include the following:

- IP Routing
- 10/100 Ethernet
- Channelized T1
- Static Routes
- Frame Relay
- Fragmentation

The border router uses the following protocols and interfaces:

- IPIP Tunnels
- IPSEC over IPIP
- Border Gateway Protocol (BGP)
- Bidirectional Forwarding Detection (BFD)
- OSPF Protocol

10.1.2 Border Router – Installation and Configuration

Prerequisites: Ensure you have the required cabling and connectors.

Process:

1. Install the border router in a rack. See S6000 Introduction, Installation, and Configuration on page 27.
2. Connect the border router to a power source. See S6000 Introduction, Installation, and Configuration on page 27.
3. If necessary, ground the border router. See S6000 Introduction, Installation, and Configuration on page 27.
4. Connect the CEN equipment to the border router. See Border Router Cabling on page 203.
5. Configure the border router. See S6000 Introduction, Installation, and Configuration on page 27.

   NOTICE: The border router is not configured or managed by UNC or UEM. Actions must be performed locally as these routers exist outside the Motorola Solutions Radio Network Infrastructure (RNI).
   In ASTRO® 25/LTE CEN systems, the Border Router requires a configuration file established manually using a text editor to meet specific requirements for each Customer Enterprise Network (CEN). See your Motorola Solutions field support representative. For details concerning Border Routers in ASTRO® 25/LTE CEN configuration see Border Router – Functional Description on page 200.

10.1.2.1 Border Router Cabling

The network cables are connected to the border router depending on the I/O modules used.

Border routers may contain appropriate modules for the WAN 1 or WAN 2 slots to accommodate network connections to your enterprise network and the RNI. For details on the S6000 router I/O modules, see Field Replaceable Units – S6000 on page 62.

NOTICE: The term UltraWAN module can refer to the UltraWAN module or the UltraWAN II module, unless otherwise specified. The UltraWAN II module (identified by the Roman numeral II in the upper right corner of the module faceplate) has been introduced to replace an obsolete component. The function of the two modules is the same.

IMPORTANT: The UltraWAN II module requires Enterprise Operating System (EOS) software version 15.4 or higher. Do not use the UltraWAN II module with EOS software version lower than 15.4, or the router may reboot continuously.

NOTICE: If you need assistance when designing Customer Network Interfaces (CNIs), contact Motorola Solutions.

If Dynamic System Resilience is implemented on your system, two border routers provide paths to a DSR Master Site pair. There are no changes in physical connections.

In the ASTRO® 25/LTE interface, a LAN port is used to connect the Border Router(s) and the LTE Primary South Router and the Primary North Router. See Border Router – Functional Description on page 200.

10.1.2.2 CEN Network Elements Operations

In Unified Event Manager (UEM), network elements in the Customer Enterprise Network (CEN) subsystem must have the IP address of the Network Address Translation (NAT) protocol configured.

The NAT IP address configuration is needed for UEM to be able to discover and manage network elements that are in the CEN subsystem.

For network elements in the CEN subsystem, a device managed resource (DMR) is created with the UEM NAT IP address instead of the UEM Radio Network Infrastructure (RNI) IP address. For network elements with subsystem different from CEN, a DMR is created with UEM RNI IP address.

You can configure single CEN network elements manually or you can configure multiple CEN network elements by loading an external NAT IP configuration file to UEM. The NAT IP configuration file is generated by Motorola Solutions Support Center (SSC) per request.

10.1.2.2.1 Configuring NAT IP for Multiple Network Elements in the CEN

Follow this procedure for expansion purposes only. In this procedure, you configure the IP address of the Network Address Translation (NAT) protocol of Customer Enterprise Network (CEN) network elements that are not managed by Unified Event Manager (UEM). Configure the NAT IP address in UEM to enable UEM to discover CEN network elements that use the NAT protocol. If the NAT IP address is not configured in UEM, UEM discovers the network elements but they do not communicate with UEM.

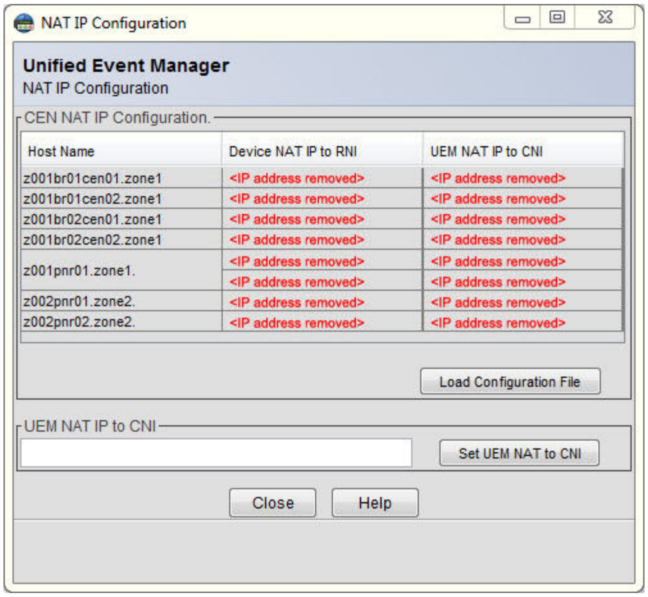
Prerequisites: Contact Solution Support Center (SSC) and request the creation of a NAT IP configuration `.xml` file.

Procedure:

1. Save the NAT IP configuration `.xml` file on a PC with network access to UEM and log on to UEM from the PC.
2. In UEM, from the main menu, select **Tools** → **Configure NAT IP**.
3. In the **NAT IP Configuration** window, click **Load Configuration file**.
4. Navigate to the NAT IP configuration`.xml` file you want to load. Click **Open**.

IP addresses necessary for UEM and CEN network elements to communicate are loaded to UEM and appear in the **NAT IP Configuration** window.

Figure 61: NAT IP Configuration Window



Host Name	Device NAT IP to RNI	UEM NAT IP to CNI
z001br01cen01.zone1	<IP address removed>	<IP address removed>
z001br01cen02.zone1	<IP address removed>	<IP address removed>
z001br02cen01.zone1	<IP address removed>	<IP address removed>
z001br02cen02.zone1	<IP address removed>	<IP address removed>
z001pnr01.zone1.	<IP address removed>	<IP address removed>
	<IP address removed>	<IP address removed>
z002pnr01.zone2.	<IP address removed>	<IP address removed>
z002pnr02.zone2.	<IP address removed>	<IP address removed>

Postrequisites: Discover reconfigured network elements to ensure correct communication with UEM.

1 If the reconfigured network elements are already discovered, delete them from UEM.

2 Discover the reconfigured network elements. See Discovering a Router in UEM on page 266.

10.1.2.2.2
Configuring NAT IP for a Single Network Element in the CEN

Follow this procedure to configure the IP address of the Network Address Translation (NAT) protocol of single Customer Enterprise Network (CEN) network elements that Unified Event Manager (UEM) manages. Configure the NAT IP address in UEM to enable UEM to discover CEN network elements that use the NAT protocol. If the NAT IP address is not configured in UEM, UEM discovers the network elements but they do not communicate with UEM.

Procedure:

1 From the main menu, select **Tools** → **Configure NAT IP**.

2 In the **UEM NAT IP to CNI** field, type the IP address of the network element you want to configure. Click **Set UEM NAT to CNI**.

IP addresses necessary for UEM and CEN network elements to communicate are loaded to UEM and appear in the **NAT IP Configuration** window.

Postrequisites: Discover reconfigured network elements to ensure correct communication with UEM.

1 If the reconfigured network elements are already discovered, delete them from UEM.

2 Discover the reconfigured network elements. See Discovering a Router in UEM on page 266.

10.1.3
Border Router – Maintenance and Troubleshooting

For maintenance and troubleshooting information, see S6000 Introduction, Installation, and Configuration on page 27. Generic maintenance and troubleshooting applies, except that the Border Router is not configured or managed by UNC or UEM. Actions must be performed locally as these routers exist outside the Motorola Solutions Radio Network Infrastructure (RNI).

Border Router Failures: In case of a Border Router failure, the link between the CEN and the RNI is lost. If a redundant Border Router is present in the system, losing one link does not cause the connection to the RNI to be lost.

Border Router Communication Failures: If the Border Router in the Unified Event Manager (UEM) has a communication failure, one potential reason is the router had a configuration change and the maximum number of registered managers may have been reached. To successfully re-manage the router in this situation, it is necessary to clear the registered SNMP managers. See “ResetV3” in the *Enterprise OS Software Reference Guide* manual.

10.2
Peripheral Network Router

This section contains information specific to the S6000 when used as a Peripheral Network Router.

10.2.1
Peripheral Network Router – Functional Description

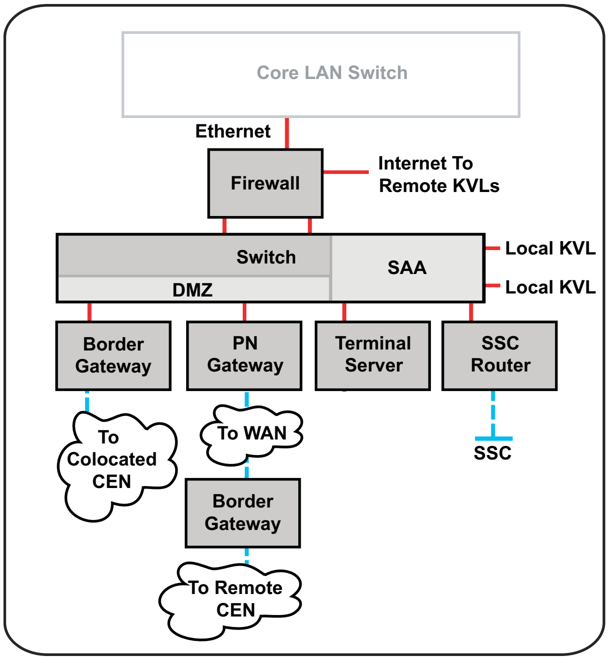
Peripheral network routers expand border router access capability to the peripheral network for your enterprise network.

Peripheral network routers provide data communication support for the IV&D radio communication network and HPD applications. Peripheral network routers are Motorola Solutions Network Router (MNR) S6000 routers that may include UltraWAN (ST6010) or UltraWAN II (ST6017) modules, as well as ST6011 FlexWAN modules. The modules in the WAN 1 and WAN 2 slots accommodate your network connections to the enterprise network and the peripheral network, respectively. For systems with Ethernet (IPv4 or IPv6) connectivity between the peripheral network routers and border routers, the third Ethernet port is used for WAN connectivity.

The peripheral network router resides outside the firewall in the De-Militarized Zone (DMZ) to route traffic between the Motorola Solutions Radio Network Infrastructure (RNI) and a Customer Enterprise Network (CEN). The router supports a peripheral network at the DMZ created in the RNI-DMZ firewall. The peripheral network router can be configured to use network address translation (NAT) or IP tunneling for secure routing of traffic.

If Dynamic System Resilience is implemented on your system, more than one peripheral network router may be used to support data traffic based on your system configuration. See the *Dynamic System Resilience* manual for details.

Figure 62: Peripheral Network Router – System Context



S_Firewall_Option_With_Switch_B

NOTICE: The peripheral network router is shown connected to the DMZ switch.
In the diagram, the box labeled **Ethernet LAN Switches** is located in the zone core of the radio network infrastructure.

10.2.1.1
Peripheral Network Router – EOS Functions

A certain list of interfaces, protocols, basic routing, and IP features in the Enterprise OS (EOS) is used by the peripheral network router.

The peripheral network router uses basic routing and IP features in the Enterprise OS (EOS) software including the following:

- IP Routing
- 10/100 Ethernet
- Channelized T1
- Static Routes
- Frame Relay

- Fragmentation

The peripheral network router uses the following protocols and interfaces:

- Point to Point Protocol (PPP)
- Multicast
- Type of Service (TOS)
- Dynamic Host Configuration Protocol (DHCP)
- Network Time Protocol (NTP)
- Simple Network Management Protocol (SNMP)

10.2.2 Peripheral Network Router – Installation and Configuration

Prerequisites: Prepare the required cabling and connectors.

Process:

1. Install the peripheral network router in a rack. See S6000 Introduction, Installation, and Configuration on page 27.
2. Connect the peripheral network router to a power source. See S6000 Introduction, Installation, and Configuration on page 27.
3. If necessary, ground the peripheral network router. See S6000 Introduction, Installation, and Configuration on page 27.
4. Connect the CEN equipment to the peripheral network router. See Peripheral Network Router Cabling on page 207.
5. Configure the peripheral network router.

   NOTICE: The peripheral network router is not configured or managed by UNC or UEM. Actions must be performed locally as these routers exist outside the Motorola Solutions Radio Network Infrastructure (RNI).

10.2.2.1 Peripheral Network Router Cabling

The network cables are connected to the peripheral network router depending on the I/O modules used.

For details on the S6000 router I/O modules, see Field Replaceable Units – S6000 on page 62. The peripheral network router has a 100Base-TX connection to the DMZ switch to support the routing of traffic between devices in the DMZ.

IMPORTANT: The UltraWAN II module requires Enterprise Operating System (EOS) software version 15.4 or higher. Do not use the UltraWAN II module with EOS software version lower than 15.4, or the router may reboot continuously.

NOTICE: The term UltraWAN module can refer to the UltraWAN module or the UltraWAN II module unless otherwise specified. The UltraWAN II module (identified by the Roman numeral II in the upper right corner of the module faceplate) has been introduced to replace an obsolete component. The function of the two modules is the same.
If you need assistance when designing Customer Network Interfaces (CNIs), contact Motorola Solutions.

If Dynamic System Resilience is implemented on your system, more than one peripheral network router may be used, however there are no changes in physical connections.

10.2.3 Peripheral Network Router – Maintenance and Troubleshooting

Generic maintenance and troubleshooting procedures apply, except that the Peripheral Network Router is not configured or managed by UNC or UEM. Actions must be performed locally as these routers exist outside the Motorola Solutions Radio Network Infrastructure (RNI). For maintenance and troubleshooting information, see S6000 Introduction, Installation, and Configuration on page 27.

Chapter 11

ASTRO 25 Centralized Conventional Sites

This chapter provides information on the S2500 router in ASTRO® 25 system conventional architectures.

11.1 Conventional RF Site Router (S2500)

The conventional RF site router is used at conventional only sites that are remote from the system’s zone core.

11.1.1 Conventional RF Site Router – Functional Description

The conventional RF site router is used at conventional only sites that are remote from the system's zone core. Conventional only sites are standalone sites that have routers and CCGWs with conventional base stations/repeaters.

The following configurations are supported for a Conventional Only site router:

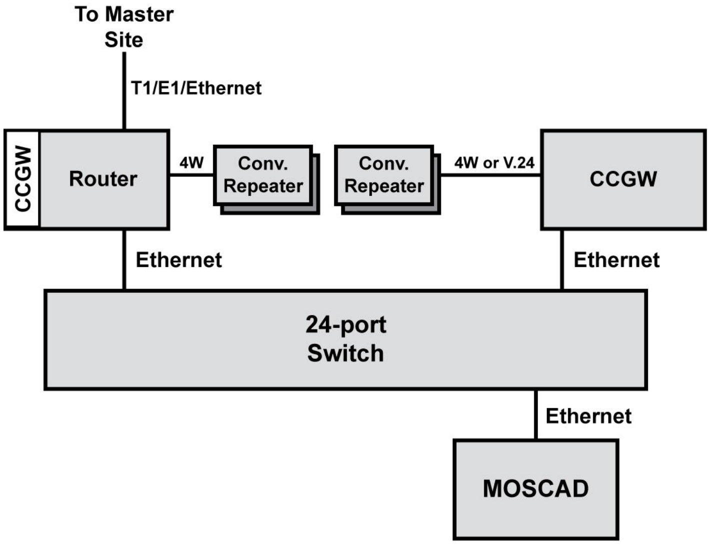
- Remoted through a single site link
- Remoted through dual site links (requires at least three routers – two acting as site routers and one acting as a CCGW). In a site configured with dual site links, CCGW cannot be integrated with the site router.
- Colocated at the core

A Conventional Only Site is considered a console site, but a special type of console site that has no consoles.

CCGW can be a standalone device or CCGW capabilities can coexist with the routing functionality on the site router. Conventional RF Site routers can also host conventional channels if they include the V.24 (for digital connectivity) or E&M modules (for analog connectivity).

The following figure shows the architecture for a Conventional Only site with a single site link. Here, the RF site router acts as both a router and CCGW.

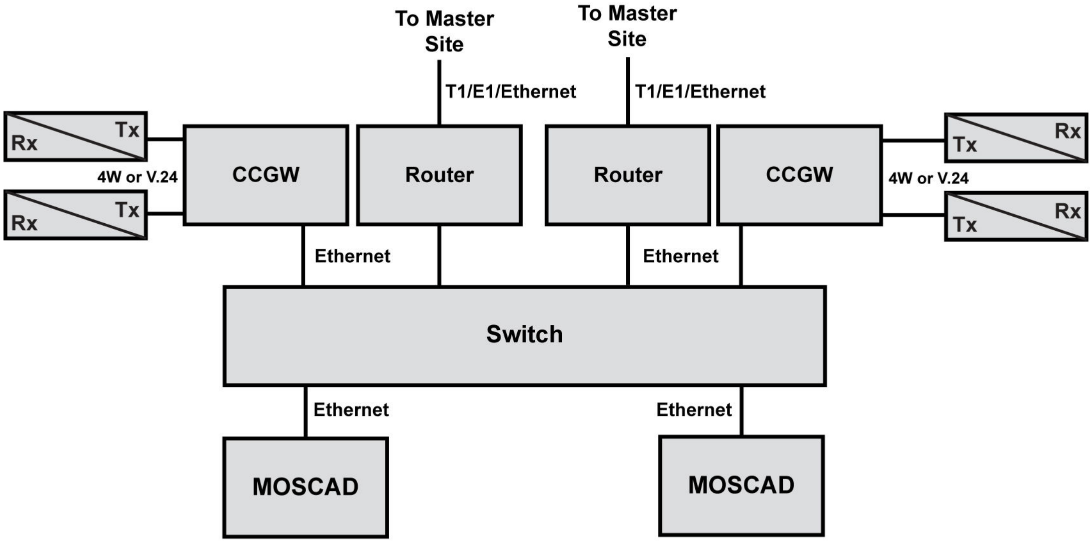
Figure 63: Conventional Only Site with a Single Site Link



conv_site_config_single

The following figure shows the architecture for a Conventional Only site with dual site links. Here, three routers are required, two acting as site routers and one acting as a CCGW.

Figure 64: Conventional Only Site with Dual Site Links



conv_site_config_dual

11.1.2 Conventional RF Site Router – Installation and Configuration

Prerequisites: Prepare the required cabling and connectors.

Process:

1 Install the Conventional RF site router in a rack. See S2500 Introduction, Installation, and Configuration on page 66.

2 Connect the Conventional RF site router to a power source. See S2500 Introduction, Installation, and Configuration on page 66.

3. If necessary, ground the Conventional RF site router. See S2500 Introduction, Installation, and Configuration on page 66.
4. Connect the equipment to the Conventional RF site router. See Conventional RF Site Router Cabling on page 211.
5. Configure the Conventional RF site router. See S2500 Introduction, Installation, and Configuration on page 66.

11.1.2.1 Conventional RF Site Router Cabling

The Conventional RF site router and other devices are connected at a conventional only site to support ASTRO® 25 Conventional channel resources.

The conventional site router cabling depends on whether the Conventional Only site is:

- Remoted through a single site link
- Remoted through dual site links (requires at least three routers – two acting as site routers and one acting as a CCGW)

Table 80: Conventional RF Site Router Cable Connections

From Router		To Destination Device		
Port	**Connector type**	**Port**	**Connector type**	**Description**
LAN 1	RJ-45	Port 1, Ethernet LAN Switch	RJ-45	Communications connection between the S2500 conventional site router and the Ethernet LAN switch.
I/O Module A (T1/E1)	RJ-45	T1 or E1 from carrier	RJ-45	This T1/E1 link connects the conventional only site through the router to the master site. A T1/E1 I/O module (ST2512) must be installed in the S2500 to make this connection.
Ethernet 10Base-T module (Port 2) (if using Flexible Ethernet Site Links)	RJ-45	Ethernet backbone	RJ-45	This link exists between the router and the Ethernet backbone. An ST2510 Ethernet module must be installed in slot A of the S2500 to make this connection for Flexible Ethernet links.
I/O Module B, Digital Module	V.24 (RJ-45)	Base Station	RJ-45	Use these connections when the conventional RF site router is used as a digital CCGW to support ASTRO® 25 Conventional channel resources.
Analog Module	E&M (RJ–1CX)	Base station	N/A	Use these connections when the conventional RF

From Router		To Destination Device		
Port	Connector type	Port	Connector type	Description
				site router is used as an analog CCGW.

For more details on Flexible Ethernet site links, see the *Flexible Site and InterZone Links* manual.

See the customized cabling and configuration information provided by Motorola Solutions for port connections specific to your system.

11.1.3 Conventional RF Site Router – Maintenance and Troubleshooting

Generic maintenance and troubleshooting procedures apply. For maintenance and troubleshooting information, refer to S2500 Introduction, Installation, and Configuration on page 66.

11.2 Conventional Channel Gateway (CCGW)

The Conventional Channel Gateway (CCGW) provides an interface between the console and the base station. CCGW can be a standalone device or CCGW capabilities can coexist with the routing functionality on the site router.

11.2.1 CCGW – Functional Description

The following configurations are supported for a Conventional Only site:

- Remoted through a single site link
- Remoted through dual site links (requires at least three routers – two acting as site routers and one acting as a CCGW)
- Colocated at the core

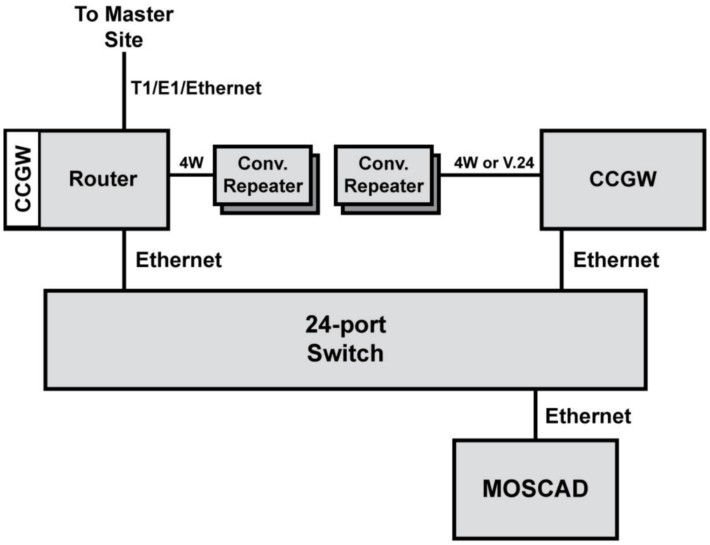
For Analog Conventional, CCGW provides call detection, vocoding and devocoding of audio, station keying and dekeying through Tone Remote Control (TRC) or E&M relay, and tone Line Operated Busy Light (LOBL) detection for parallel console interoperation.

For ASTRO® 25 Conventional, CCGW interfaces to a base station through the ASTRO Infrastructure Signaling (AIS) protocol. CCGW supports digital conventional voice calls and packet data in secure coded, or clear modes at the base station.

In addition, CCGW provides an interface to the zone controller through the X-Zone Infrastructure Signaling (XIS) protocol.

The following figure shows the architecture for a Conventional Only site with a single site link. Here, the RF site router acts as both a router and CCGW.

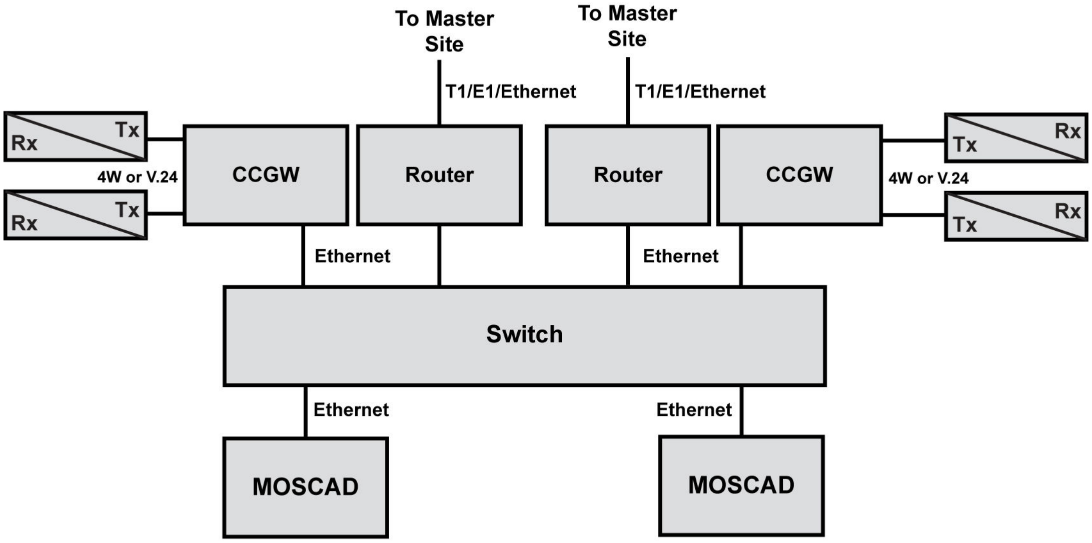
Figure 65: Conventional Only Site with a Single Site Link



conv_site_config_single

The following figure shows the architecture for a Conventional Only site with dual site links. Here, three routers are required, two acting as site routers and one acting as a CCGW.

Figure 66: Conventional Only Site with Dual Site Links



conv_site_config_dual

See the “Conventional Channel Gateway Utilization” in the *GGM 8000 System Gateway* manual for additional information about CCGWs.

11.2.1.1
Adding a CCGW to an Existing Site

When conventional operation functionality is added to an existing site, a CCGW must be added to the infrastructure of the site.

A CCGW can be added to an existing site in the following ways:

- Add a hardware kit to existing S2500 site routers, which enables them to act as site routers and as CCGWs.
- Upgrade existing routers to S2500 routers that include the hardware kit.
- Add a dedicated CCGW, which includes the hardware kit (this device acts strictly as a gateway device).

NOTICE: A CCGW can be equipped with both analog and digital modules; however, a CCGW can function in only one mode. The S2500 routers must be Version B or higher (model number ST2500B or higher) in order to accept the hardware kit. The model number is shown on the rear of the router.

11.2.1.2
Analog CCGW Introduction

For Analog Conventional, a hardware kit adds four 4W interface ports to CCGW. Conventional base stations or comparators connect directly or indirectly to these interface ports. Analog Conventional supports parallel console operations through Tone Remote Control and tone Line Operated Busy Light (LOBL) detection.

11.2.1.3
Digital CCGW Introduction

For ASTRO® 25 Conventional, a V.24 module adds two V.24 digital interface ports to CCGW. Base stations or comparators connect directly to these interface ports.
ASTRO® 25 Conventional channels support parallel console operations only through ASTRO-TAC 3000 Comparators and the 3.1 Coexistence feature.

11.2.1.4
Conventional Operation Characteristics

Consider:

- In a multizone capable system, use GGM 8000 as CCGW for conventional channels that can be accessed by consoles in another zone.
- In a site configured with dual site links, CCGW cannot be integrated with the site router.
- Up to four Analog Conventional, or up to two ASTRO® 25 Conventional base stations or comparators may be connected to a single CCGW. If the number of stations or comparators at a site exceeds the capacity of CCGW, additional CCGWs are added to support them.

  NOTICE: Instead of adding additional CCGWs, the GGM 8000 Gateway could also be used. The GGM 8000 Gateway is required in order for the system to support the maximum capacity of conventional channels.
- Base stations interface directly or indirectly to CCGW.
- Conventional sites (CCGWs) can be mixed at any location in the system, analog or digital.

11.2.1.5
Role of CCGW

CCGW provides an interface to the network for:

- Conventional call-processing functions
- Vocoding/Devocoding 4W analog to G.728 IP packets
- Translation between AIS and XIS protocol for V.24 digital audio
- Multicasting of audio over the network

- Analog call detection
- Station control
- LOBL detection
- Outbound digital voice/packet data/signaling/station control contention

NOTICE: G.728 is an International Telecommunications Union (ITU) standard for coding telephone bandwidth speech that was designed to provide speech quality equivalent to or better than that of previous standards. G.728 coding is well suited to a wide range of applications, including both voice storage and voice communications, and performs well in the presence of multiple speakers and background noise.

11.2.1.6

CCGW Interfaces

CCGW acts a gateway between various site devices and the rest of the system. The CCGW translates voice and data into the format needed for each individual site type. CCGWs are capable of supporting digital or analog channel types

11.2.1.6.1

Digital CCGW with V.24 Module

Digital CCGW (DCCGW) is an S2500 site router configured with one or two V.24 modules.

The router has software installed and supports the V.24 interface for digital audio. The software added allows for communications with the zone controller to facilitate digital call transmissions to and from MCC 7500 Dispatch Console(s). The zone controller has responsibility for call assignments involving digital conventional dispatch from an MCC 7500 Dispatch Console.

NOTICE: A Digital CCGW is defined by the Provisioning Manager as a Conventional Site with Site Type = **Digital**. If a GGM 8000 is to be used for analog and digital conventional channels, it should be configured with Site Type = **Combination**, as this represents a GGM 8000 CCGW and allows for greater flexibility in configuring the conventional site.

Up to two digital conventional sources may be connected to an S2500 router.

NOTICE: For two digital sources to be connected, two V.24 modules must be installed in the S2500 router.

11.2.1.6.2

Analog CCGW with E&M Module

The Analog CCGW is an S2500 site router configured with the conventional-to-IP interface kit (4-port E&M module and DSP SIMM).

The router has software installed and supports the 4-wire E&M interface for analog audio. The software added allows for communications with the zone controller to facilitate analog call transmissions to and from MCC 7500 Dispatch Consoles. The zone controller has responsibility for call assignments involving analog conventional dispatch from an MCC 7500 Dispatch Console. The Analog CCGW only supports analog-only conventional channels. The S2500 router configured as an Analog CCGW does not support MDC 1200 conventional channels, mixed mode channels, or ACIM channels.

NOTICE: An Analog CCGW is defined by the User Configuration Manager as a conventional site with Site Type = **Analog**. If a GGM 8000 is to be used for analog and digital conventional channels, it should be configured with Site Type = **Combination**, as this represents a GGM 8000 CCGW and allows for greater flexibility in configuring the conventional site.

11.2.1.7 Analog Conventional-to-IP Interface Kit

The Analog Conventional-to-IP Interface Kit adds four 4W E&M interface ports and a DSP SIMM to the S2500 router. The E&M ports on the S2500 router connect to the analog audio ports on a base station, or sometimes to a comparator. The ports are connected either directly using simple cabling, or indirectly through pairs of channel banks that are interconnected through lease lines. Because the termination impedance for audio signals is changed at each port (between standard 600–Ohm impedance and 10K-Ohm high impedance), more than one receiving device is connected on the same line.

An S2500 router that is outfitted with the Conventional-to-IP interface kit and the appropriate system software is referred to as a CCGW. The software that comes with the Conventional-to-IP interface hardware kit enables CCGW to receive inbound digitized 16–bit PCM audio signals through the E&M module, compress them, and convert them to G.728 audio packets. The router forwards the G.728 audio packets through the LAN/WAN ports for radio and parallel console transmissions. For outbound audio, the router decompresses the packetized audio received through the LAN/WAN ports and sends the decompressed audio to the E&M module for conversion back to analog audio.

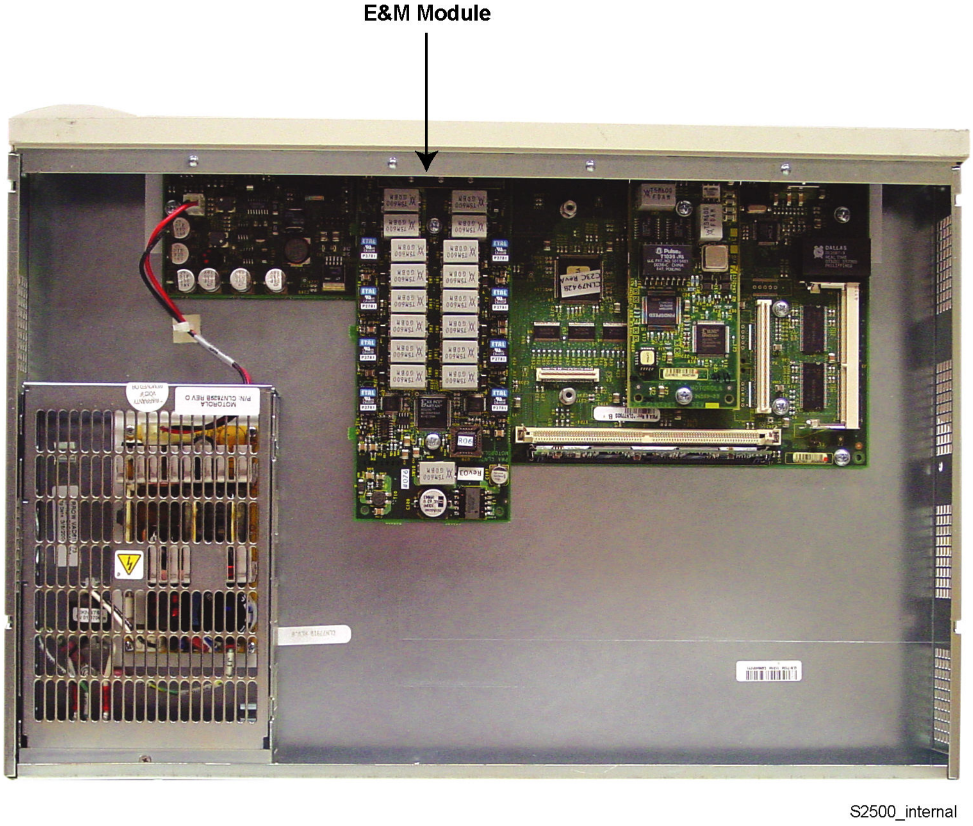
Control signals are handled separately from audio signals. One side of the E&M interface controls the state of the E-lead and monitors the state of the M-lead, while the other side controls the state of the M-lead and monitors the state of the E-lead.

IMPORTANT: The relay/switch function on the CCGW E&M port is provided on the E-lead, and the relay closure detection function is provided on the M-lead. Many pieces of network equipment having E&M port interfaces reverse this naming convention.

NOTICE: The logical states of either the E-lead or the M-lead correspond to whether electrical current is flowing through the leads.

The following figure shows the inside of an S2500 router that contains the Conventional-to-IP Interface Kit.

Figure 67: CCGW with Conventional-to-IP Interface Kit



11.2.1.8
V.24 Module

The V.24 module adds two V.24 digital interface ports to the S2500 router. Base stations connect directly or indirectly through external modems to these ports.

An S2500 router that is outfitted with the V.24 module and the appropriate system software is referred to as a digital CCGW. The software that comes with the V.24 module enables the digital CCGW to receive inbound digital audio into IP audio and control packets and forward audio packets using Improved Multi-Band Excitation (IMBE) /Advanced Multi-Band Excitation (AMBE) speech compression algorithms. The router forwards the IMBE/AMBE packets through the LAN/WAN ports for radio and parallel console transmissions. For outbound audio, packets received by the router are converted to V.24 format and sent to the digital ASTRO station, receiver, or comparator.

11.2.1.9
Link Redundancy

Each CCGW is considered by the fault management system to be an independent logical site (that is, a logical conventional site). When there is one or more CCGW located at a console site, each CCGW and the console site establishes its own control path with the zone controller. Control paths are logical links created to facilitate reliable communications between a zone controller and various system elements. For each system element (For example, CCGW), there are two control paths created for redundancy: an active path and a standby path. CCGW maintains a redundant pair of paths, regardless of where it is colocated.

The pair of control paths between CCGW and the zone controller are:

- **ZC-CCGW control path** – The zone controller view of the control path with CCGW.

- **CCGW-ZC control path** – CCGW view of the control path with the zone controller.

Having a view of both ends of these control paths from a fault management perspective aids in diagnosis and troubleshooting. The control paths are fault-managed in their own container. The control paths are designed to minimize bandwidth usage. Both single-site and dual-site link architectures are supported for improved availability.

11.2.2 CCGW – Installation and Configuration

Prerequisites: Prepare the required cabling and connectors.

Process:

1. Install CCGW in a rack. See S2500 Introduction, Installation, and Configuration on page 66.
2. Connect CCGW to a power source. See S2500 Introduction, Installation, and Configuration on page 66.
3. If necessary, ground CCGW. See S2500 Introduction, Installation, and Configuration on page 66.
4. Connect the equipment to CCGW. See the following topics for more information:
   - Connecting the Digital CCGW Directly to a Base Station on page 225
   - Connecting the Digital CCGW to a Modem on page 226
   - Connecting the Digital CCGW to a Subrate Data (SRU) Card on page 227
   - Connecting CCGW to the LAN Switch on page 228
   - CCGW Cabling on page 230
5. Configure CCGW. See S2500 Introduction, Installation, and Configuration on page 66.

11.2.2.1 Software Installation

No additional software programs need installing, in addition to the software installed as part of the routine installation procedures. CCGW ships with all the necessary software pre-installed. This includes both the MNR ASTRO® Smart/Zone Software Upgrade and the Enterprise Operating System (EOS).

EOS enables the router to coexist as a CCGW, and enables CCGW to be configured for conventional operation. Conventional operation is achieved by executing commands that are contained in a configuration file (boot.cfg) that is executed when the router is booted up. Once these commands have been executed, EOS initializes CCGW, enabling it to communicate with the Network Management system LDAP service. EOS configures the CCGW based on the LDAP configuration.

A CCGW configuration file (CCGWDB) is created on the EOS flash. This file contains the latest CCGW configuration from the network management LDAP server. It is updated when changes are received from the Network Management LDAP server after CCGW router has been rebooted and is used for boot-up persistence. If CCGW cannot communicate with the LDAP server, it attempts to read the configuration from the EOS flash.

11.2.2.2 Vocoder Hardware to Router

Install the Vocoder hardware kit that adds CCGW capabilities to the S2500 router. The S2500 router can be outfitted for Analog Conventional or ASTRO® 25 Conventional CCGW operation.

11.2.2.3 Analog Base Stations to CCGW

The analog base stations are physically connected to CCGW through one or more of the four 4W E&M interface ports. The E&M interface is configured to operate in E&M Type II mode. While the base stations do not specifically implement a standard E&M interface, they do include all of the components (voltage supplies, relays, and current detectors) needed to interoperate with one.

In E&M Type-II mode, the two line control functions are implemented with two current loops. Each side of an E&M Type-II connection has a relay, a voltage source, and a current detector. The relay/switch function in the CCGW E&M interface is provided on the E and SG signals. The E and SG signals are connected to a voltage source and an optically isolated current detector on the Base Station, to form a current loop controlled by the CCGW. The Base Station detects CCGW relay closure with its current detector. The contacts of the Base Station controlled relay are interconnected with the M and SB signals on CCGW, to form a current loop that is controlled by the Base Station. The CCGW SB signal provides the voltage source for the current loop and the current detector (on the CCGW M-Lead) detects when relay closure occurs on the Base Station.

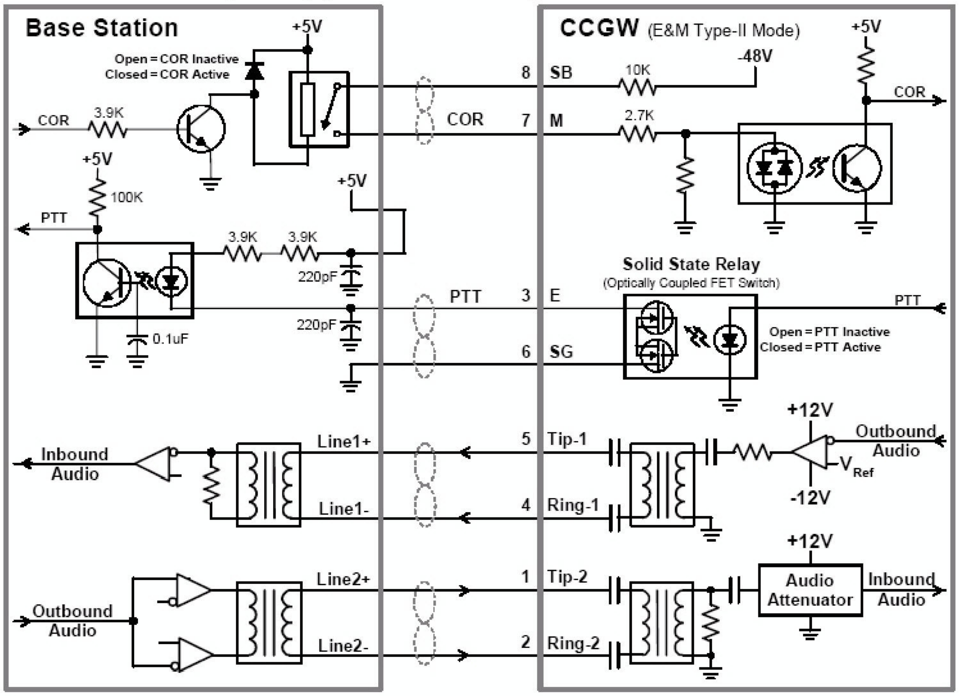
CCGW provides four 8-pin RJ-45 ports (per device) that connect to analog conventional base stations. Each port contains the following inputs and outputs:

- 600 Ohm – 10K Ohm, balanced analog audio input - Used to accept radio audio from the base station
- 600 Ohm – 10K Ohm, balanced analog audio output - Used to send console transmit audio to the base station
- Input buffer - Used to detect Carrier Operated Relay (COR) closure in the base station
- 1 Amp, 24 VDC relay output - Used for relay keying of the base station

The most common application for CCGW involves the interconnection of the Analog Conventional ports on a base station across a WAN to an MCC 7500 Dispatch Console. In the most straightforward implementation, the Analog Conventional ports on CCGW are directly connected to the Analog Conventional ports on a base station. The following figure shows the recommended wiring scheme for directly connecting a CCGW to a QUANTAR® base station through the Analog Conventional ports. For the specific port number on the base station that is used to connect the 4W interface cable, refer to the documentation supplied with the particular base station.

Note that while the drawing shows a 5 Volt supply output on the Base Station as the voltage source for the current detector on the Base Station, CCGW safely accepts any voltage source between ±60 VDC. However, the voltage output of the source must not cause the optically isolated current detector on the Base Station to exceed its maximum current rating.

Figure 68: CCGW E&M Port Connection with Base Station



S2500_EM_Port_interconnections_w_QUANTAR

NOTICE: It may be necessary to connect additional circuitry to accommodate various unique base station applications.

The Relay/Switch Closure Detection function provided on pins 7 and 8 and the Relay/Switch function provided on pins 3 and 6 is only possible if the equipment connected is colocated on the same premises as CCGW. Please note that the relay/switch function on the CCGW E&M port is provided on the E signal line and the relay closure detection function is provided on the M signal line: which is the reverse of the naming conventions used on most if not all the equipment used in ASTRO® 25 networks having E&M port interfaces.

The control signal pairs are designed to interoperate with E&M signals meeting the TIA/EIA-464 specification. According to specification TIA/EIA-464, the voltages on the line control signals must adhere to the following limits:

- The continuous working voltages on the E&M line control signals signal must not exceed 60 V in magnitude (nominal working voltage is –48 VDC)
- Transient peaks of up to 300 V are permitted (for inductive or capacitive ringing)
- A level of 80 V is sustained for no more than 10 ms

CAUTION: The analog interface of CCGW is designed to connect directly to analog stations that are physically located in the same room or building, or through a connection provided by a microwave link. If analog lines are used to connect CCGW to an analog station at another location, a primary surge suppression device must be installed.

11.2.2.3.1
Pin Functions for Analog Base Station Connections to CCGW

The following table describes pin functions for analog base station connections to CCGW.

Table 81: Pin Functions for Analog Base Station Connections to CCGW

Pin Function	Description
Relay/Switch Closure Detection (Pins 7 and 8)	Pins 7 and 8 are normally used as part of a current loop that is controlled by the attached equipment. Pin 8 provides a current-limited –48 VDC supply to drive the current loop, while pin 7 detects when the relay/switch on the attached equipment is closed. The current detector on pin 7 detects currents of 2 mA or greater and is used in circuits with average signal levels ranging between ±60 V. The Thyristor Surge Protection Devices (not shown) that are included in this circuit trigger when the signal significantly exceeds 60 V in magnitude and as a result contribute to the overall signal settling time for signals exceeding 60 V.
Relay/Switch Function (Pins 3 and 6)	Pins 3 and 6 are normally used to control (open and close) a current loop that is monitored by the attached equipment. CCGW uses a solid-state relay to control the current loop. The solid-state relay on the CCGW switches as much as 1 A. However the current through pins 3 and 6 should not average more than 0.5 A, or significantly exceed 1 A peak, else the self-healing polymer “fuses” (not shown) that are included in this circuit triggers. The average voltage level must not exceed 60 V in magnitude for much longer than 10 ms, to avoid damaging the Transient Voltage Suppressors (not shown) in the circuit. The solid-state relay has a worst-case off-state leakage current of 10 µA, when open. Pins 3 and 6 are not protected against high voltage. If your particular application warrants it, however, you may add your own surge protection devices.
Outbound Audio (Pins 4 and 5)	The analog audio from CCGW is carried (differentially) on pins 4 and 5. The source impedance of the outbound audio circuit is 600 Ohms and the receiving end of the line is terminated with a load impedance of 600 Ohms (to maintain specified output gain levels). It is recommended that the terminators on the receiving equipment be configured appropriately, if multiple termination options are available. The outbound audio circuit is designed to drive an analog audio tone with average levels as high as +11 dBm (±3.9 V peak-to-peak) into a 600 Ohms load without clipping. Transient Voltage Suppressors on the secondary side of the isolation transformer will clip signals significantly exceeding 8 V (differential) and Thyristor Surge Protection Devices on the primary side of the transformer trigger when the differential voltage significantly exceeds 25 V.
Inbound Audio (Pins 1 and 2)	The analog audio into CCGW is carried (differentially) on pins 1 and 2. Normally CCGW is configured to provide a termination impedance of 600 Ohms across these pins. CCGW has a software option (referred to as the high-impedance option, the non-terminated option, or, alternatively, the 10K–Ohms loading option) to disconnect the terminating load, on a port-by-port basis, for cases where another piece of equip-

Pin Function	Description
	ment (attached to the same signal pair) is configured to provide the 600 Ohms termination. **NOTICE:** The resulting termination impedance is greater than 10K–Ohms. The inbound audio circuit is designed to receive an analog audio tone with average levels as high as +11 dBm (±3.9 V peak-to-peak) without clipping. Transient Voltage Suppressors on the secondary side of the isolation transformer will clip signals significantly exceeding 8 V (differential) and Thyristor Surge Protection Devices on the primary side of the transformer trigger when the differential voltage significantly exceeds 25 V.

11.2.2.4

Digital Base Stations to Digital CCGW

The S2500 V.24 module supports two V.24 serial ports. The ports on the V.24 module are labeled “Port 1” and “Port 2”. However, the MNR S2500 software reserves port 2 or 3, A and B for ASTRO® 25 Conventional V.24 ports.

Consider:

- If the V.24 module is installed in **port 2 (I/O slot A)**, then the software uses **port numbers 2A and 2B**.
- If the V.24 module is installed in **port 3 (I/O slot B)**, then the software uses **port numbers 3A and 3B**.

NOTICE: You can install the V.24 module in either I/O slot A or I/O slot B; however, the software supports only one V.24 module per S2500.

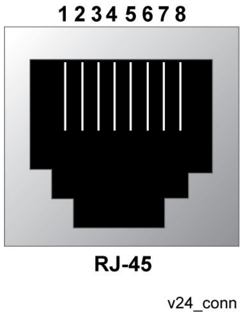
Cabling the V.24 ports depends on the device being connected to the digital CCGW.

- To connect directly to a base station, review the figures in Digital CCGW to a Base Station Signal Diagrams on page 223 and perform the procedure in Connecting the Digital CCGW Directly to a Base Station on page 225.
- To connect to a modem, review the figures in Digital CCGW to a Modem Signal Diagram on page 225 and perform the procedure in Connecting the Digital CCGW to a Modem on page 226.
- To connect to a Subrate Data (SRU) card, review the figure in Digital CCGW to SRU Signal Diagram on page 226 and perform the procedure Connecting the Digital CCGW to a Subrate Data (SRU) Card on page 227.

In addition, you must ensure that the clock source is set appropriately. For details, see Setting the Clock Source in the Provisioning Manager on page 227.

The following figure illustrates the pin locations on the S2500 V.24 connector.

Figure 69: S2500 V.24 Connector (RJ-45)



NOTICE: The pin functions described in the following table apply to internal clock applications (co-located links with direct connections to a base station). When configuring the digital CCGW for an external clock application (external links connected through a modem or SRU), an external clock signal (TCLK-EXT) must be brought in on pin 2 of the digital CCGW V.24 port interface. For details, see Connecting the Digital CCGW to a Modem on page 226 or Connecting the Digital CCGW to a Subrate Data (SRU) Card on page 227.

The following table lists the pin functions.

Table 82: S2500 V.24 Connector Pin Functions

Pin Number	Name
1	RCLK – Receive Clock (in)
2	CD – Carrier Detect (in)
3	TCLK– Transmit Clock (out)
4	GND (Signal Ground)
5	RxD – Receive Data (in)
6	TxD – Transmit Data (out)
7	CTS – Clear to Send (in)
8	RTS – Request to Send (out)

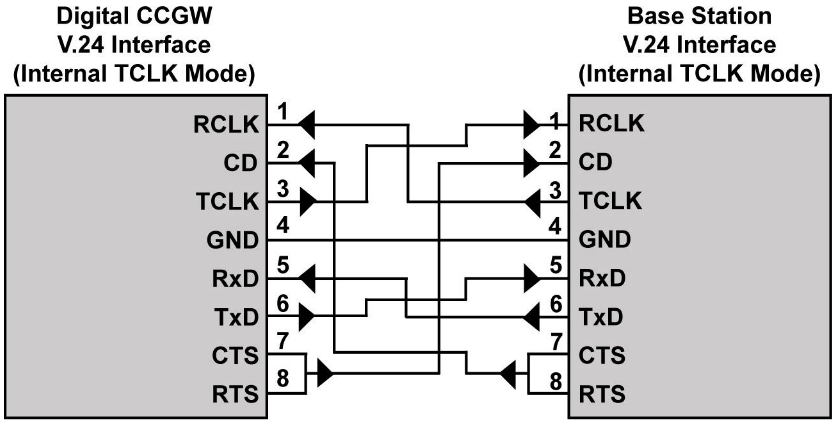
11.2.2.4.1
Digital CCGW to a Base Station Signal Diagrams

This section describes the V.24 interface to a base station.

If connecting an S2500 V.24 connector directly to a base station, connect the S2500 to the base station using a port-to-port (V.24 null modem) cable with RJ-45 plugs at both ends.

NOTICE: The interface interconnection illustrated in Figure 70: Signal Diagram: Digital CCGW V.24 Interface to Base Station on page 224 can also be achieved by using the pre-built cable designed for use with the MNR S2500 V.24 module (part number DKN6143A-A).

Figure 70: Signal Diagram: Digital CCGW V.24 Interface to Base Station

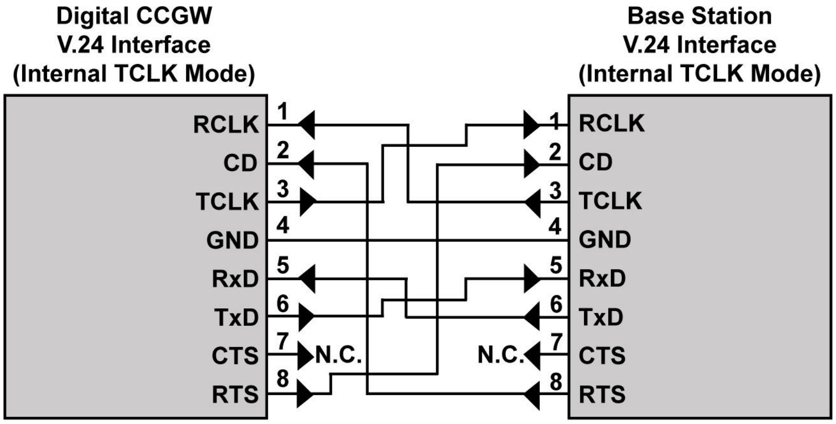


DCCGW_to_BR_pinout

Alternatively, you can connect the S2500 to the base station using a port-to-port (V.24 null modem) cable with RJ-45 plugs at both ends and wired as illustrated in Figure 71: Alternative Signal Diagram: Digital CCGW V.24 Interface to Base Station on page 224.

NOTICE: The interface interconnection illustrated in the following figure can also be achieved by using a pre-built cable, such as the Motorola Solutions colocated ASTRO-TAC null cable (part number 30C83271X14).

Figure 71: Alternative Signal Diagram: Digital CCGW V.24 Interface to Base Station



DCCGW_to_BR_alt_pinout

In addition to interconnecting the digital CCGW and the base station as illustrated in the figures, follow these best practice recommendations to ensure that the port clock is configured appropriately:

CAUTION: Incorrect settings cause data bit errors that damage the link packets and result in packet loss with the data transfers to and from the digital CCGW.

- Configure the V.24 port interface on the digital CCGW to synchronize the transmission of its serial data (TXD) using an internally-generated reference clock.
- Configure the V.24 port interface on the base station to synchronize the transmission of its serial data (TXD) using an internally-generated reference clock.
- Connect the transmit clock output signal (TCLK) from the V.24 port of one device to the receive clock input signal (RCLK) on the V.24 port of the other device.

Both of the V.24 ports use the transmit clock signal supplied by the other device to synchronize the reception of serial data.

11.2.2.4.2 Connecting the Digital CCGW Directly to a Base Station

Prerequisites: Prepare the required cabling and connectors.

When and where to use: Perform this procedure to connect the S2500 V.24 module.

Procedure:

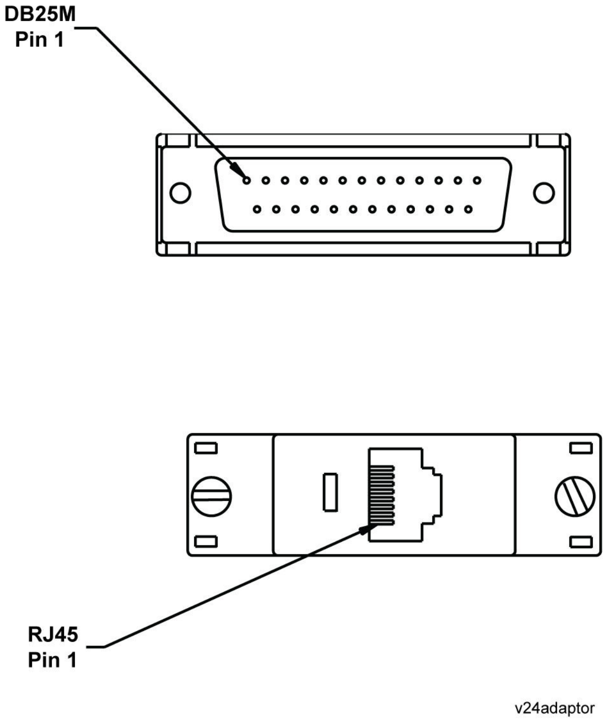
1. Attach one end of a port-to-port (V.24 null modem) cable to the Digital CCGW V.24 port.
2. Attach the other end of the V.24 null modem cable to the base station port.

11.2.2.4.3 Digital CCGW to a Modem Signal Diagram

If connecting the S2500 V.24 connector to a modem, attach an RJ-45- to-25-pin “D” cable adapter to the modem port.

Figure 72: RJ45-to-25 “D” Cable Adapter Pin Locations Connect on page 225 shows the pin locations for the cable adapter.

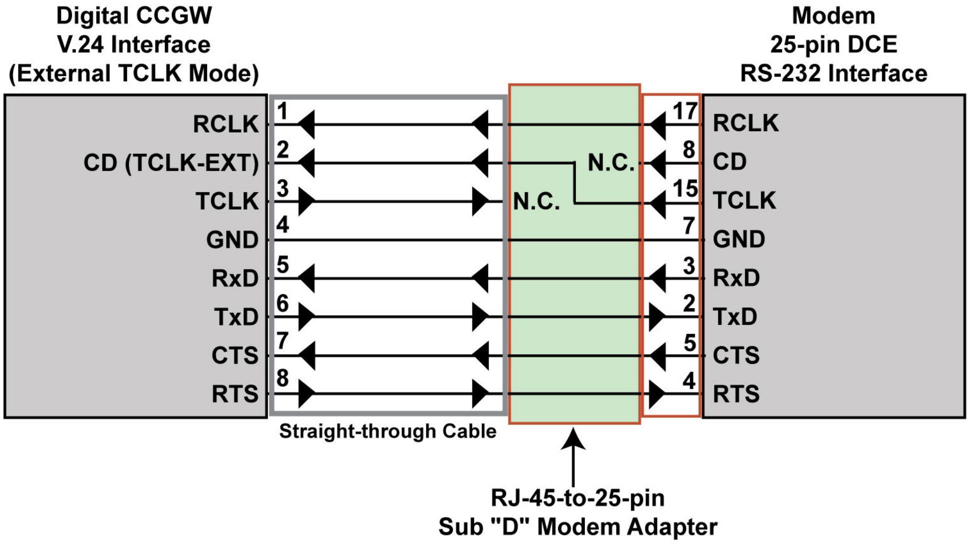
Figure 72: RJ45-to-25 “D” Cable Adapter Pin Locations Connect



Connect the S2500 V.24 connector to the modem adapter using a straight-through cable wired as illustrated in Figure 73: Signal Diagram: Digital CCGW V.24 Interface to Modem (With Cable Adapter) on page 226.

NOTICE: The interface interconnection illustrated in the following figure can also be achieved by using a pre-built cable, such as Motorola Solutions part number 58D82653X45.

Figure 73: Signal Diagram: Digital CCGW V.24 Interface to Modem (With Cable Adapter)



DCCGW_to_Modem_pinout

In addition to interconnecting the Digital CCGW and the modem, follow these best practice recommendations to ensure that the port clock is configured appropriately:

CAUTION: Incorrect settings cause data bit errors that damage the link packets and result in packet loss with the data transfers to and from the Digital CCGW.

- Configure the DB-25 interface connection on the modem to supply both the transmit and the receive clock signals to the V.24 port interface on the Digital CCGW.
- Configure the V.24 port interface on the Digital CCGW to use the externally-supplied clock signal from the modem to synchronize the transmission of serial data.
- Connect the TCLK-EXT input signal on the V.24 port interface on the Digital CCGW to the TCLK output signal on the DB-25 interface connection on the modem.

11.2.2.4.4

Connecting the Digital CCGW to a Modem

Prerequisites: Prepare the required cabling and connectors.

When and where to use: Perform this procedure to connect the S2500 V.24 module.

Procedure:

1. Attach an RJ45-to-25-pin “D” cable adapter (CLN8488A) to the modem port.
2. Attach one end of an RJ45-to-RJ45 straight-through cable to the Digital CCGW V.24 port.
3. Attach the other end of the RJ45-to-RJ45 straight-through cable to the cable adapter on the modem port.

11.2.2.4.5

Digital CCGW to SRU Signal Diagram

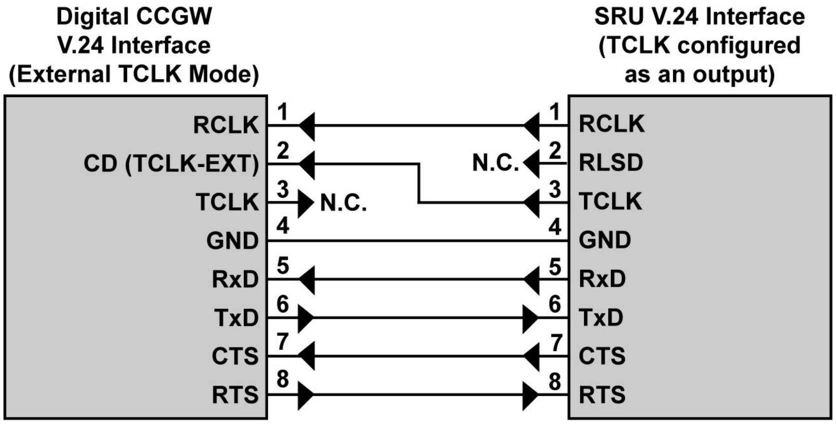
This section shows the V.24 connection to an SRU card.

If connecting an S2500 V.24 connector to an SRU card, connect the two ports using an 8-conductor cable with standard RJ-45 plugs at both ends and wired as illustrated in Figure 74: Signal Diagram: Digital CCGW V.24 Interface to SRU on page 227.

CAUTION: The two ends of the cable are not interchangeable and should be marked accordingly.

NOTICE: The interface interconnection illustrated in the following figure can also be achieved by using the Motorola Solutions Digital CCGW-to-SRU modular adapter (part number SP0201001).

Figure 74: Signal Diagram: Digital CCGW V.24 Interface to SRU



DCCGW_to_SRU_pinout

In addition to interconnecting the Digital CCGW to the SRU as illustrated in the figure, follow these best-practice recommendations to ensure that the port clock is configured appropriately:

CAUTION: Incorrect settings cause data bit errors that damage the link packets and result in packet loss with the data transfers to and from the Digital CCGW.

- Configure the V.24 port interface on the SRU to supply both the transmit and the receive clock signals to the V.24 port interface on the Digital CCGW.
- Configure the V.24 port interface on the Digital CCGW to use the externally-supplied clock signal from the SRU to synchronize the transmission of serial data.
- Connect the TCLK-EXT input signal on the V.24 port interface on the Digital CCGW to the TCLK output signal on the V.24 port interface on the SRU.

11.2.2.4.6 Connecting the Digital CCGW to a Subrate Data (SRU) Card

Prerequisites: Prepare the required cabling and connectors.

When and where to use: Follow these steps to install and configure the router.

Procedure:

1. Attach the appropriate end of the 8-conductor cable to the Digital CCGW V.24 port.
2. Attach the other end of the 8-conductor cable to the SRU card port.

11.2.2.4.7 Setting the Clock Source in the Provisioning Manager

Interconnect the devices and follow best-practice recommendations to configure the clock mode on the Digital CCGW V.24 ports.

Consider:

- If you connect Digital CCGW directly to a base station, the clock source for the V.24 communication link should be set to **internal** (the transmit clock is generated internally in the Digital CCGW).

- If you connect Digital CCGW to a modem, the clock source for the V.24 communications link should be set to **external** (the transmit clock is generated by an external device; in this case, the modem).
- If you connect Digital CCGW to a subrate data (SRU) card, the clock source for the V.24 communications link should be set to **external** (the transmit clock is generated by an external device; in this case, the SRU card).

You configure the clock source in Provisioning Manager. From the Provisioning Manager main window, select the **Zone** object, choose **Conventional Site**, select **CCGW**, then select the **Conventional Channel (Conventional Site)** object.

The Clock Source parameter is on the **Digital Conventional Setup** tab. For details, see the Provisioning Manager manual.

IMPORTANT: A reboot is required in order for changes made in Provisioning Manager to be adopted permanently by the Digital CCGW.

11.2.2.5

Connecting CCGW to the LAN Switch

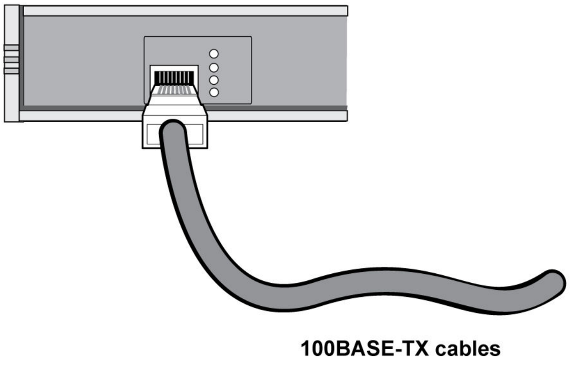
The S2500 router supports one or two Ethernet (LAN) connectors, depending on whether the router is configured with the optional 10Base-T module. Connect CCGW to the LAN switch to cable the 10Base-T/ 100Base-TX Ethernet connectors on the base system or the 10Base-T Ethernet connector on the optional 10Base-T module.

Prerequisites: Prepare the required cabling and connectors.

Procedure:

1 Connect one end of a 10Base-T or 100Base-TX cable to the LAN port on the front panel (left end) of the S2500.

Figure 75: LAN Port on CCGW



CCGW_LAN_port

NOTICE: To cable the Ethernet port on the base system for a 100Base-TX connection, you must use a 100Base-TX cable.

2 Connect the other end of the cable to the Ethernet device.

11.2.2.6

CCGW – Configuration

You perform certain steps to configure CCGW in an ASTRO® 25 system. To add a CCGW to a new or existing site, contact Motorola Solutions field personnel to initiate the request to perform the initial setup with the Motorola Solutions Support Center (SSC). Once the SSC has completed the initial device setup, you can proceed with the Provisioning Manager configuration of CCGW. During the initial configuration, the SSC assigns an instance ID to CCGW; this ID must match the CCGW ID configured through Provisioning Manager, and you must obtain this information before the configuration through Provisioning Manager can occur.

NOTICE: If the device ID and the Provisioning Manager-configured ID do not match, conventional is inoperable.

11.2.2.6.1
Configuring CCGW at an MCC 7500 Dispatch Console (NM/Dispatch) Site

CCGWs are located as part of the MCC 7500 Dispatch Console site and reside on the subnet for the MCC 7500 Dispatch Console site. Individual CCGWs are assigned an IP address on the subnet, and the host part of the IP address is determined through the uniquely assigned CCGW ID configured from the Provisioning Manager. The CCGW ID has a valid range of 1-10. The CCGW ID must be assigned uniquely to the CCGWs for each MCC 7500 Dispatch Console site to avoid the same IP address being assigned to two or more CCGWs. This implies the following rules must be enforced by system administrators:

```
CCGW IP Address = 10.zone.NMDispConv.CCGW ID+84 (i.e. 10.1.1.85 for CCGW ID
= 1, zone = 1, NMDispConv = MCC 7500 Site ID-1000 = 1001-1000 = 1)
```

In this example, **NMDispConv** is the physical site number.

To add a CCGW to a new or existing site, the Motorola Solutions Support Center (SSC) assigns an instance ID to CCGW during initial device setup. This ID must match the CCGW ID that you configure by using Provisioning Manager.

NOTICE: If the device ID and the Provisioning Manager-configured ID do not match, conventional is inoperable.

For CCGWs co-located at the trunked RF sites (Trunking Repeater Site or Simulcast Prime), the host part of the IP address remains the same except that there can be up to two CCGWs co-located at the trunked RF sites, so the CCGW ID should be chosen to be unique in the range of 1-2.

11.2.2.6.2
Audio Levels Configuration for the Analog CCGW

CCGW analog conventional channel audio level parameters are listed in the *Console Sites* and *Conventional Operations* manual. The audio level parameters must be configured separately for each analog channel in CCGW. These parameters are configured through Provisioning Manager.

NOTICE: Digital Conventional devices do not require level settings.

CCGW parameters include outbound and inbound path parameters. Outbound path parameters include:

Outbound Alignment Tone Level
This parameter controls the analog output level from the CCGW channel.

Average Outbound G.728 Audio Level
This parameter tells the CCGW the average audio level coming from the consoles.

CCGW Inbound Path Parameters

The CCGW’s inbound path parameter includes an AGC whose operation is controlled by:

Average Inbound G.728 Audio Level
This parameter tells CCGW the target audio level going to the consoles. This is the target output level of the CCGW’s inbound AGC.

Inbound AGC Knee Setting
The knee setting of the CCGW channel’s inbound AGC controls the channel’s receive sensitivity.

Inbound AGC Type

This can be configured as either DLM or Pure AGC. DLM means that the AGC gain adjustment is only active when the AGC detects voice activity.

11.2.2.7

Comparator to CCGW

If an optional comparator is being used, connect the interface cable from the comparator to one of the four 4W analog ports or to one of the two V.24 digital ports on the front panel of CCGW.

11.2.2.8

CCGW Cabling

CCGWs are connected to other devices at a conventional only site to support ASTRO® 25 Conventional channel resources.

The CCGW cabling depends on whether the Conventional Only site is:

- Remoted through a single site link
- Remoted through dual site links (requires at least three routers – two acting as site routers and one acting as a CCGW)

NOTICE: The CCGWDB file is refreshed from the LDAP server. When a router is replaced, the LDAP server is the source for refreshing the CCGWDB file.

Table 83: CCGW Cable Connections

From CCGW		To Destination Device		
Port	**Connector type**	**Port**	**Connector type**	**Description**
LAN 1	RJ-45	Port 1, Ethernet LAN Switch	RJ-45	Communications connection between the S2500 conventional site router and the Ethernet LAN switch.
I/O Module A, Digital Module	V.24 (RJ-45)	Base Station	RJ-45	Used when the conventional RF site router is used as a digital CCGW to support ASTRO® 25 Conventional channel resources.
Analog Module	E&M (RJ–1CX)	Base station	N/A	Used when the conventional RF site router is used as an analog CCGW.

NOTICE: Refer to the customized cabling and configuration information provided by Motorola Solutions for port connections specific to your system.

See “Cabling the E&M (Analog) Connectors” in Chapter 2 of the *Motorola Network Router (MNR) S2500 Hardware User Guide* for additional cabling and pinout information.

11.2.3 CCGW – Maintenance and Troubleshooting

Generic maintenance and troubleshooting procedures apply. For maintenance and troubleshooting information, refer to S2500 Introduction, Installation, and Configuration on page 66.

11.2.3.1 CCGW Diagnostics

Diagnostics are remote commands initiated by a Network Management user that allow the user to enable a server or process, disable a server or process, or force a download of configuration parameters. Following are the diagnostic commands that control CCGW. These do not apply to a site router that is not configured as CCGW. They do not impact the routing functionality of the site router when CCGW coexists on the same device.

- Enable of CCGW
- Disable of CCGW
- Enable of each channel at CCGW
- Disable of each channel at CCGW

11.2.3.2 CCGW Serviceability

The CCGW serviceability interface enables technicians to view and query logged information and to enable/disable system/device options. Access to the serviceability interface may be either local (through a local configuration management terminal) or remote.

See the MCC 7500 manuals and *Conventional Operations* manuals for the information that is accessible through the CCGW serviceability interface.

11.2.3.3 Troubleshooting CCGW with Network Management Components

You can use the following network management applications to troubleshoot the CCGWs:

ZoneWatch

ZoneWatch data that is specific to conventional calls is noted in the MCC 7500 manuals and *Conventional Operations* manual. For a full discussion of the use of ZoneWatch for troubleshooting, refer to the ZoneWatch documentation.

Affiliation Display

Affiliation Display data that is specific to conventional calls is noted in the MCC 7500 manuals and *Conventional Operations* manual. For a full discussion of the use of Affiliation Display for troubleshooting, see the Affiliation Display documentation.

Air Traffic Router

The messages from the ATR that are specific to conventional calls are noted in the MCC 7500 manuals and *Conventional Operations* manual. For a full discussion of the use of ATR for troubleshooting, refer to the Air Traffic Router documentation.

11.2.3.4 Failures Reported

The following types of failures for conventional are reported to the fault management system through SNMP:

- Link failures:

  - CCGW links (control paths) to and from the zone controller (ZC), that is ZC-CCGW CP and CCGW-ZC CP
  - Console site link (control path) to ZC
  - CCGW link to LAN switch
- CCGW internal failures
- Digital link loss between CCGW and digital capable RF equipment

Internal failures in CCGW (for example, DSP, E&M, or v.24 module failures) are reported to the fault management system as if they were failures of the conventional channel, although the reason code in the trap indicates the actual module that failed.

11.2.3.4.1 Conventional Gateway to Zone Controller

Each CCGW maintains an independent control link with the zone controller. If two or more CCGWs are located at an RF site, the link between each CCGW and the zone controller is reported independently. Failures of a CCGW to ZC and ZC to CCGW control link are detected and reported in two ways. In the event of a failure of the link, the failure is detected within 10 seconds during the periods of inactivity and within 1.5 seconds when there is an active voice call (inbound or outbound) on any of the conventional channels served by CCGW. The same is true when a Conventional Site Controller is managing CCGW.

11.2.3.4.2 CCGW to GTR 8000/GPW 8000

CCGW detects a link failure with a GTR 8000/GPW 8000. Any voice calls active on the link during a link failure end immediately when the link is lost. The channel is displayed as failed after a short period of time. This time window allows for the link to encounter a brief burst of link errors or microwave fades that may cause lost packets without flashing link failures too frequently to system operators.

11.2.3.4.3 GCM 8000 to GTR 8000/GPW 8000

The GCM 8000 detects a link failure with GTR 8000 and GPW 8000 at a voted subsite. Any outbound voice calls active on the channel during a sub-site failure continue on other subsites, and any inbound calls may be voted on other active subsites. The sub-site is displayed as failed after a short period of time. This time window allows for the link to encounter a brief burst of link errors or microwave fades that may cause a lost packets without flashing link failures too frequently to system operators. Note that sub-site link failures may result in the sub-site entering Fall Back In-Cabinet Repeat mode if that feature is used.

If the link between CCGW and GCM 8000 fails, detection follows the same rules as for CCGW to GTR 8000 and GPW 8000 links.

11.2.4 CCGW – Reference

This section contains tables for E&M module analog connector pinouts and path to port syntax rules.

11.2.4.1 E&M Module Analog Connector Pinouts

Table 84: E&M Module Analog Connector Pinouts

Pin	Analog Connector Pinouts
1	Tip-2 (Receive audio in +)
2	Ring-2 (Receive audio in –)
3	E-lead
4	Ring-1 (Transmit audio in –)
5	Tip-1 (Transmit audio in +)
6	Signal ground (SG)
7	M-lead
8	Signal battery (SB)

11.2.4.2 S2500 Path-to-Port Syntax Rules for the E&M Module

Table 85: E&M Module – S2500 Path-to-Port Syntax Rules

Interface	Path-to-Port Syntax	Syntax Description
E&M analog connectors	*<n>*	*<n>* = 4, 5, 6 or 7 E&M ports 4, 5, 6, and 7 on the S2500 correspond to conventional channels 1, 2, 3, and 4 with the following mapping: • Port 4 – Chan 1 • Port 5 – Chan 2 • Port 6 – Chan 3 • Port 7 – Chan 4

11.2.4.3 V.24 Module Digital Connector Pinouts

Table 86: V.24 Module Digital Connector Pinouts

Pin	Digital Connector Pinouts
6	TD – Transmit Data (out)
5	RD – Receive Data (in)
8	RTS – Request to Send (out)
7	CTS – Clear to Send (in)

Pin	Digital Connector Pinouts
4	GND (Signal Ground)
3	TCLK – Transmit Clock (out)
2	CD – Carrier Detect (in)
1	RCLK – Receive Clock (in)

See also Table 82: S2500 V.24 Connector Pin Functions on page 223 for additional details of connection types.

11.2.4.4 S2500 Path-to-Port Syntax Rules for the V.24 Module

Interface	Path-to-Port Syntax	Syntax Description
V.24 digital connectors	***<nA>*** and ***<nB>***	***<n>*** = 2 or 3 V.24 paths/ports 2A and 2B or 3A and 3B map to digital conventional channels 1 and 2 with the following mapping: • Port 2A -> Channel 1 • Port 2B -> Channel 2 • Port 3A-> Channel 1 • Port 3B -> Channel 2

Chapter 12

ASTRO 25 Interoperability

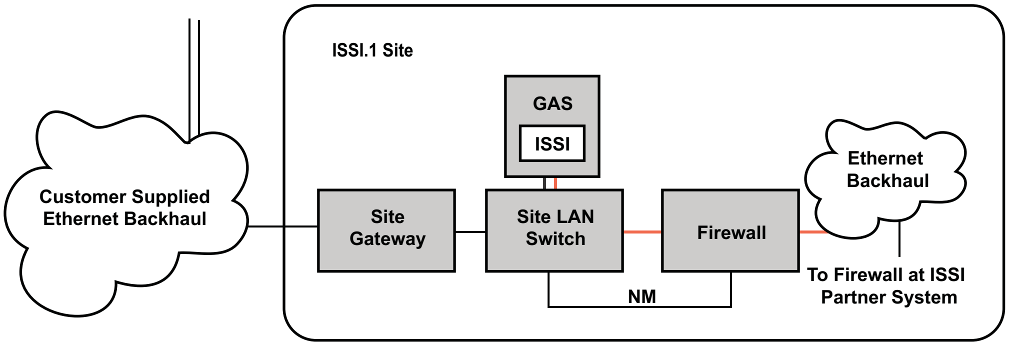
This chapter provides information on the S2500 router used at the ISSI.1 site.

12.1 Site Router (ISSI.1) – Functional Description

The site router is used at the ISSI.1 site to interface to the master site core router. If more than one ISSI.1 site gateway application is installed on the Generic Application Server at the site, each of the applications requires its own dedicated site router link.

The ISSI.1 Network Gateway communicates with the site router through the site LAN switch by establishing an IP session to each router. The site router directs all voice, control, and network management traffic between the master site and the remote site. Control and voice are logically separated and routed to separate endpoints in the zone core. The site router connection to the ASTRO® 25 system network is the same as an RF site router, and is managed as such.

Figure 76: ISSI.1 Site



S_ISSI_GW_L_System_Option_A

12.2 Site Router (ISSI.1) – Installation and Configuration

Prerequisites: Prepare the required cabling and connectors.

Process:

1. Install the ISSI.1 site router in a rack. See S2500 Introduction, Installation, and Configuration on page 66.
2. Connect the ISSI.1 site router to a power source. See S2500 Introduction, Installation, and Configuration on page 66.
3. If necessary, ground the ISSI.1 site router. See S2500 Introduction, Installation, and Configuration on page 66.
4. Connect the equipment to the ISSI.1 site router. See Site Router (ISSI.1) Cabling on page 236.
5. Configure the ISSI.1 site router. See S2500 Introduction, Installation, and Configuration on page 66.

12.2.1 Site Router (ISSI.1) Cabling

Table 87: Site Router (ISSI.1) Cable Connections to Other Devices

From Router		To Destination Device		
Port	Connector type	Port	Connector type	Description
LAN 1	RJ-45	Port 1, Ethernet LAN Switch	RJ-45	Communications connection between the S2500 ISSI.1 site router and the Ethernet LAN switch.
I/O Module A (T1/E1)	RJ-45	T1 or E1 from carrier	RJ-45	This T1/E1 link connects the ISSI.1 site through the router to the master site. A T1/E1 I/O module (ST2512) must be installed in the S2500 to make this connection.
Ethernet module (Port 2) (if using Flexible Ethernet Site Links)	RJ-45	Ethernet back-bone	RJ-45	This link exists between the router and the Ethernet back-bone. Ethernet module (ST2510) must be installed in slot A of the S2500 router to make this connection for Flexible Ethernet links.

NOTICE: To connect the site to the master site, either the T1/E1 or Ethernet module is used. For more details on Flexible Ethernet site links, see the *Flexible Site and InterZone Links* manual.
See the customized cabling and configuration information provided by Motorola Solutions for port connections specific to your system.

The MNR S2500 router is used for the ISSI.1 Network Gateway. For every S2500 router, an I/O module should be used.

- If the S2500 router is connected using a T1/E1 site link, a T1/E1 module (ST2512) is required.
- If the S2500 router is connected using an Ethernet site link, a 10BASE-T module (ST2510) is required.

12.3 Site Router (ISSI.1) – Maintenance and Troubleshooting

Generic maintenance and troubleshooting procedures apply. For maintenance and troubleshooting information, see S2500 Introduction, Installation, and Configuration on page 66.

Chapter 13

ASTRO 25 Circuit Simulcast Subsystem

This chapter provides information on the routers in an ASTRO® 25 Circuit Simulcast subsystem.

13.1 Circuit Simulcast Prime Site Router

The Circuit Simulcast Prime Site Router handles the traffic between the prime site network and the T1 link to the master site.

13.1.1 Circuit Simulcast Prime Site Router – Functional Description

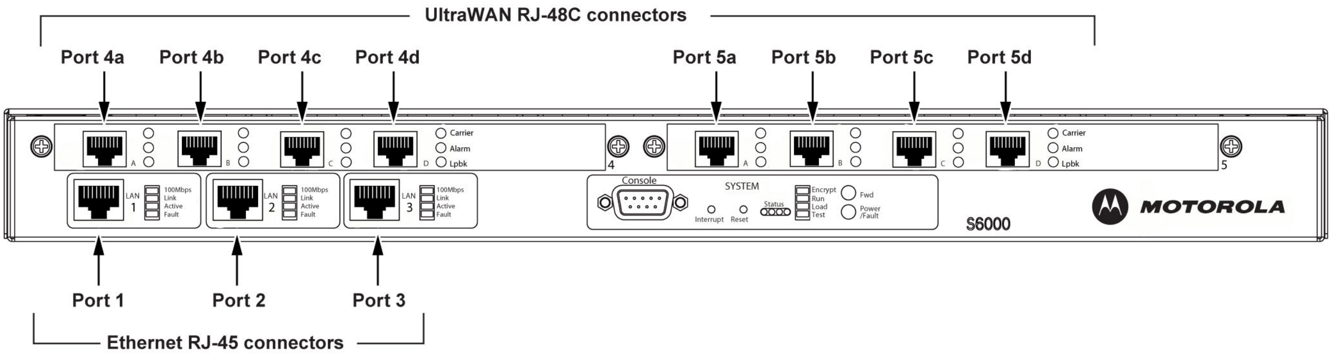
The prime site router provides a Wide Area Network (WAN) interface that carries all the traffic for the RF site including voice, control, data, and network management traffic. The router provides network connectivity for the remote sites as well as encapsulation of Ethernet Local Area Network (LAN) packets in Frame Relay Internet Protocol (IP) packets on a serial (FlexWAN) interface.

NOTICE: If the prime site router is configured for encryption, see the *Link Encryption and Authentication* manual for details about installation and configuration issues specific to router encryption.

The prime site router directs all control, voice, and network management traffic between the prime site LAN and the site link to the master site. The router connects to T1/E1 links through UltraWAN or UltraWAN II ports and connects the Ethernet LAN through a LAN port. An optional redundant prime site router can be installed in the prime site. The S6000 router with an ST6010 UltraWAN module or ST6017 UltraWAN II module is used as the prime site router.

The figure below shows the prime site router, which provides a WAN interface to carry all the traffic for the RF site including voice, data, and network management traffic.

Figure 77: Prime Site Router with Ultra WAN Modules – Front View



S6000_port_mapping_w_Ultra_WAN_modules

The router provides network connectivity to the remote sites, in addition to the following:

- Media conversion – The router converts the 100 MB Ethernet LAN packets to IP packets encapsulated in Frame Relay on a serial (UltraWAN) interface.
- Traffic prioritizing – The router applies the correct prioritizing masking to the packets leaving the site.
- Fragmentation – The router fragments large IP packets per standards.
- Dynamic Host Configuration Protocol (DHCP) service – This service allows the technician to connect to the LAN at the site using a properly configured PC with the Windows OS.

The prime site router is based on the Motorola Network Router (MNR) S6000. A built-in Ethernet port (LAN port) provides connectivity to the site Ethernet switch, where both the primary site controller and the backup site controller are accessible. If circuit-based Conventional channels are present, the UltraWAN module (ST6010) or UltraWAN II module (ST6017) provides either a T1 or E1 interface to the TeNSr channel bank WAN card.

NOTICE: The S6000 supports two versions of the UltraWAN module. The functionality of the two module versions is the same; however, the UltraWAN II module (identified by a Roman numeral “II” on the front panel), requires EOS software version 15.4 or higher.

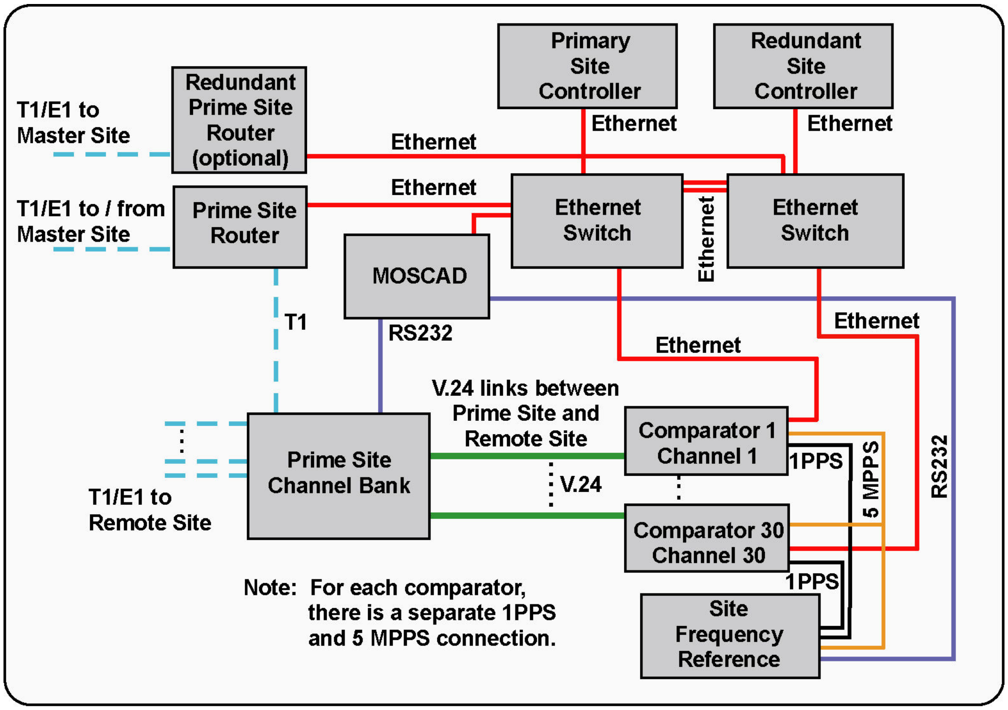
CAUTION: If you install an UltraWAN II module in an S6000 running a version of EOS software lower than the required version, the router reboots continuously.

The prime site router facilitates network management activity at the site, and provides a means of receiving and reporting the failure alarms. The Unified Network Configurator, Unified Event Manager, and MOSCAD Network Fault Management (NFM) have access to the simulcast prime site and remote sites through the prime site router.

13.1.1.1 Prime Site Router Connections

The prime site router has two UltraWAN connections to two different T1/E1 links and one Ethernet connection to one of the prime site Ethernet switches. One UltraWAN connection supports the T1/E1 link to the master site, another UltraWAN connection supports the T1/E1 link for remote site network management traffic through the channel bank, and one Ethernet port supports connection to the prime site LAN.

Figure 78: Prime Site Router – Connections



S_Simul_Prime_Site

Outbound frame relay traffic from the master site is carried over a Permanent Virtual Circuit (PVC) to the prime site router. The prime site router terminates the PVC and frame relay, and then distributes audio and control traffic to the prime site LAN, where it can be processed by the site controllers or comparators. The network management traffic intended for the remote site is passed directly over T1/E1 to the prime site channel bank.

The audio and control traffic intended for the zone core is sent to the prime site router over the prime site LAN. The prime site router encapsulates the traffic into frame relay and delivers the traffic over the T1/E1 link to the master site.

If circuit-based Conventional channels are supported in the subsystem, the site configuration is slightly different. The prime site router delivers frame relay traffic over T1/E1 through the channel bank, which multiplexes circuit-based Conventional channels and the traffic into separate timeslots and delivers the channelized T1/E1 to the master site.

13.1.1.2
Prime Site Router – EOS Functions

A certain list of interfaces, protocols, basic routing, and IP features in the Enterprise OS (EOS) is used by the prime site router.

The prime site router uses basic routing and IP features in the Enterprise OS (EOS) software including the following:

- IP Routing
- 10/100 Ethernet
- Channelized T1
- Unchannelized T1

- Static Routes
- Frame Relay
- Fragmentation

The prime site router uses the following protocols and interfaces:

- Simple Network Management Protocol (SNMP)
- Multicast
- Type of Service (TOS)
- Dynamic Host Configuration Protocol (DHCP)
- Network Time Protocol (NTP)

13.1.2 Circuit Simulcast Prime Site Router – Installation and Configuration

Prerequisites: Prepare the required cabling and connectors.

Process:

1. Install the Circuit Simulcast prime site router in a rack. See S6000 Introduction, Installation, and Configuration on page 27.
2. Connect the Circuit Simulcast prime site router to a power source. See S6000 Introduction, Installation, and Configuration on page 27.
3. If necessary, ground the Circuit Simulcast prime site router. See S6000 Introduction, Installation, and Configuration on page 27.
4. Connect the equipment to the Circuit Simulcast prime site router. See Circuit Simulcast Prime Site Router Cabling on page 240.
5. Configure the Circuit Simulcast prime site router. See S6000 Introduction, Installation, and Configuration on page 27.

13.1.2.1 Circuit Simulcast Prime Site Router Cabling

Table 88: Cable Connections from the Simulcast Prime Site Router

From Prime Site Router		Destination Device		
Port	**Connector Type**	**Port**	**Connector Type**	**Description**
LAN 1	RJ-45	Port 1, Prime Site Switch 1	RJ-45	Connection to the prime site switch.
LAN 2	RJ-45	Port 1, Switch 1 of the colocated remote site	RJ-45	Connection to the colocated RF site.
Port 4B	T1/E1, UltraWAN/ RJ48c	Channel Bank, Interface Wide Area Network (WAN) Card	T1/E1, UltraWAN/ RJ48c	T1/E1 connection to remote sites for management traffic.
Port 4C	T1/E1, UltraWAN/ RJ48c	Channel Bank, Interface WAN Card	T1/E1, UltraWAN/ RJ48c	T1/E1 connection to remote sites for conven-

From Prime Site Router		Destination Device		
Port	Connector Type	Port	Connector Type	Description
				tional audio and other site traffic.
Port 4D	T1/E1, UltraWAN/ RJ48c	Channel Bank, Interface WAN Card	T1/E1, UltraWAN/ RJ48c	T1/E1 connection to remote sites for conventional audio and other site traffic.
Port 5A	T1/E1, UltraWAN/ RJ48c	Channel Bank, Interface WAN Card	T1/E1, UltraWAN/ RJ48c	T1/E1 connection to remote sites for conventional audio and other site traffic.
Port 5B	T1/E1, UltraWAN/ RJ48c	Channel Bank, Interface WAN Card	T1/E1, UltraWAN/ RJ48c	T1/E1 connection to remote sites for conventional audio and other site traffic.
Port 5C	T1/E1, UltraWAN/ RJ48c	Channel Bank, Interface WAN Card	T1/E1, UltraWAN/ RJ48c	T1/E1 connection to remote sites for conventional audio and other site traffic.
Port 5D	T1/E1, UltraWAN/ RJ48c	Channel Bank, Interface WAN Card	T1/E1, UltraWAN/ RJ48c	T1/E1 connection to remote sites for conventional audio and other site traffic.

NOTICE: If a redundant router is being used, LAN 1 in the second router is connected to Port 1 on Switch 2.

13.1.3

Circuit Simulcast Prime Site Router – Maintenance and Troubleshooting

Generic maintenance and troubleshooting procedures apply. For maintenance and troubleshooting information, see S6000 Introduction, Installation, and Configuration on page 27.

13.2

Circuit Simulcast Remote Site Router

The Circuit Simulcast Remote Site Router handles traffic between the remote site network and the T1 link to the prime site.

13.2.1

Circuit Simulcast Remote Site Router – Functional Description

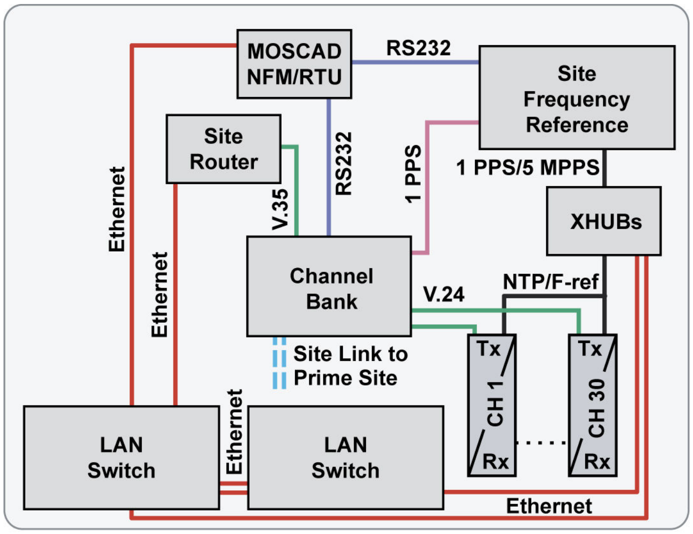
In a circuit simulcast remote site, the remote site router transports the site network management information to and from Unified Network Configurator, Unified Event Manager, and MOSCAD Network

Fault Management (NFM) servers. The remote site router connects directly to the TeNSr channel bank High Speed Unit (HSU) card through the FlexWAN/V.35 interface. The Local Area Network (LAN) port is connected to the Ethernet switch where the base radio and MOSCAD RTU are also connected.

The S2500 remote site router handles traffic between the remote site network and the T1 link to the prime site. The remote site router distributes network management traffic between the remote site channel bank and the equipment on the remote site network.

The following figure shows the functional components at a simulcast remote site with the GTR 8000 Expandable Site Subsystem.

Figure 79: Remote Site Router – Connections



S_Simul_Remote_Site_GTR8000_ESS

The remote site router directs network management traffic between the remote site channel bank and the remote site LAN. The remote site router has an Ethernet connection with the Ethernet switch at the remote site and a V.35 serial connection to the HSU card on the remote site channel bank. Network Management traffic from the master site flows through the prime site and out to the remote site channel bank. The remote site channel bank delivers the network management traffic over V.35 to the remote site router. The remote site router makes the network management traffic available to the equipment on the remote site LAN.

The remote site router provides a WAN interface that handles all of the traffic to and from the master site for the RF site including voice, control, data, and network management traffic. The remote site routers provide the following functions:

- **Media conversion** – The remote site router converts the 10 MB Ethernet LAN packets to IP packets encapsulated in Frame Relay on a FlexWAN connector or cable.
- **Traffic prioritizing** – The remote site router applies the correct prioritizing masking to the packets leaving the site.
- **Fragmentation** – The remote site router fragments large IP packets per standards.
- **Dynamic Host Configuration Protocol (DHCP) service** – This service allows a technician to connect to the LAN at the site using a properly configured PC with the Windows OS.

13.2.1.1 Circuit Simulcast Remote Site Router I/O Modules Functions

Table 89: Functional Description of Remote Site Router (S2500) with I/O Modules

Functional Router Description	S2500 I/O Module Slot 1 Port 2	S2500 I/O Module Slot 2 Port 3
Remote Site Router – Master Site Interface Only	ST2512	Empty
Remote Site Router – Circuit-based Conventional channel support	ST2511	Empty
Remote Site Router – Remote dispatch or Network Management (NM) Site support with Plant 911 at the master site	Empty	ST2510

NOTICE: The S2500 Remote Site Router with ST2511 FlexWAN module can be replaced with a Site Gateway (FlexWAN) device. The S2500 Remote Site Router with the ST2511 FlexWAN (V.35 serial interface) module supporting ASTRO® 25 Repeater Sites or Circuit Simulcast Remote Sites with circuit-based Conventional channels is replaced with the Site Gateway (FlexWAN) device. See “Replacing Daughterboards on the GGM 8000” section in the *GGM 8000 System Gateway* manual.

13.2.2 Circuit Simulcast Remote Site Router – Installation and Configuration

Prerequisites: Prepare the required cabling and connectors.

Process:

1 Install the Circuit Simulcast remote site router in a rack. See S2500 Introduction, Installation, and Configuration on page 66.

2 Connect the Circuit Simulcast remote site router to a power source. See S2500 Introduction, Installation, and Configuration on page 66.

3 If necessary, ground the Circuit Simulcast remote site router. See S2500 Introduction, Installation, and Configuration on page 66.

4 Connect the equipment to the Circuit Simulcast remote site router. See Circuit Simulcast Remote Site Router Cabling on page 244.

5 Configure the Circuit Simulcast remote site router. See S2500 Introduction, Installation, and Configuration on page 66.

13.2.2.1 Circuit Simulcast Remote Site Router Cabling

Table 90: Circuit Simulcast Remote Site Router Cable Connections

From Remote Site Router		Destination Device		
Port	Connector Type	Port	Connector Type	Description
LAN 1	RJ-45	Port 1, Remote Site Switch	RJ-45	Communications connection between the router and the remote site switch.
I/O Module B	FlexWAN	Channel bank HSU P1 Connector	V.35	Communications connection between the remote site router and the prime site.
Console	RS232/DB9	Console/ Terminal, Serial Port	RS232/DB9	Communications connection between the router and a console or terminal.

NOTICE: If a redundant router is being used, the LAN 1 port is connected to port 1 on Switch 2.

13.2.3 Circuit Simulcast Remote Site Router – Maintenance and Troubleshooting

Generic maintenance and troubleshooting procedures apply. For maintenance and troubleshooting information, see S2500 Introduction, Installation, and Configuration on page 66.

Chapter 14

System Routers Reference

This chapter contains reference information for the S6000 and S2500 routers.

14.1 Routers by Architecture

This section describes the router usage according to the position in the network and maps the role of the S6000 and S2500 routers with the GGM 8000 gateway equivalents.

Table 91: GGM 8000 Equivalents for S6000s and S2500s by ASTRO 25 Network Position

MNR Platform	Network Position	GGM 8000 Equivalent
S6000	IP simulcast prime site router (T1 or Ethernet links)	Site gateway **NOTICE:** The GGM 8000 replaces the MNR S6000 for all Ethernet configurations and links requiring one or two T1/E1s. If the link between the master site and the prime site requires three or more T1/E1s, an MNR S6000 must be used.
S6000	IP simulcast remote site access router (Ethernet links)	Remote site access gateway **NOTICE:** The GGM 8000 replaces the MNR S6000 for all Ethernet configurations; all T1/E1 configurations require an MNR S6000.
S6000	Trunking subsystem prime site router (Ethernet links only)	Site gateway
S6000	Trunking subsystem remote site router (Ethernet links only)	Remote site access gateway
S6000	Border router	Border gateway
S2500	Dispatch Console Site router	Site gateway
S2500	(Repeater) site router	Site gateway
S2500	ISSI.1 router	Site gateway
S2500	CCGW	Conventional Channel Gateway (CCGW)

MNR Platform	Network Position	GGM 8000 Equivalent
		NOTICE: The GGM 8000 supports four analog and four V.24 ports (when configured with an analog/V.24 interface kit or a Low Density Enhanced Conventional Gateway module) or eight analog and eight V.24 ports (when configured with a High Density Enhanced Conventional Gateway module) as opposed to the two analog and two V.24 ports supported on the MNR S2500.

In addition, the GGM 8000 supports the following functionality:

- Core Gateway – GGM 8000 combining the role of core and gateway routers.
- Site Gateway – GGM 8000 with a connection to a Wide Area Network (WAN) and **no** conventional channel interface (v.24, analog, and/or IP).
- Conventional Channel Gateway (CCGW) only
- Site and Conventional Channel Gateway – GGM 8000 with a connection to a WAN and with a conventional channel interface (v.24, analog, and/or IP).

14.2 Platform Replacement

Some routers can be substituted by a GGM 8000 replacement.

Table 92: Platform Replacement

Router Model	Router Nomenclature	GGM 8000 Replacement
S6000	Gateway router (Ethernet Links)	GGM 8000 Gateway
	Gateway router (T1/E1 Links)	No gateway equivalent
	Core router (Ethernet Links)	Core Gateway
	Core router (T1/E1 Links)	No gateway equivalent
	Exit router (Ethernet Links)	Exit Gateway
	Exit router (T1/E1 Links)	No gateway equivalent
	Exit/Core Router (Ethernet Links)	Exit/Core Gateway
N/A	No router equivalent	Core Gateway (L1/L2 Zone Core)
S6000	GGSN router (Ethernet Links)	GGSN Gateway
	GGSN router (T1/E1 Links)	No gateway equivalent
	Peripheral network router	No gateway equivalent

Router Model	Router Nomenclature	GGM 8000 Replacement
	Circuit Simulcast Prime Site router	No gateway equivalent
S2500	Circuit Simulcast Remote Site router	Site gateway
S6000	IP Simulcast Prime Site router (T1/E1 or Ethernet Links)	Site gateway **NOTICE:** The Site Gateway can be used with two or less T1 links - otherwise the S6000 Router is used.
	Trunking Subsystem (Ethernet Links only)	Site Gateway
S2500	IP Simulcast Remote Site router	Site gateway
S6000	IP Simulcast remote site access router (T1/E1 or Ethernet Link)	Remote site access gateway **NOTICE:** The Site Gateway can be used as a Remote Site Access Router for Ethernet links from Prime Site to Remote Site. No GGM 8000 equivalent for using a Remote Site Access Router with T1 links.
	IP Simulcast remote site access router (T1/E1 Link)	No gateway equivalent
	Trunking Subsystem remote site access router (Ethernet Link only)	Remote site access gateway
S2500	Dispatch Console Site router	Site gateway
	Repeater Site router	
	ISSI.1 router ISSI.1 site router	
S6000	Border router	Border gateway
S2500	CCGW	Conventional Channel Gateway (CCGW)
S2500	Analog CCGW LAN Analog CCGW	
	ASTRO 25 CCGW V.24 CCGW Digital CCGW LAN Digital CCGW	
N/A	No router equivalent	Conventional Channel Gateway (CCGW) **NOTICE:** Used for IP Conventional Channel Interface

Chapter 15

System Routers Disaster Recovery

This chapter provides references and information that enable you to recover a site or zone router in the event of failure.

NOTICE: Zone routers include core, exit, core/exit, gateway, and GGSN routers.

15.1

Recovering Site/Zone Routers – Non-Hardened Systems

Prerequisites: If necessary, contact your system administrator to obtain the following items:

- IP address
- Account logins and passwords
- Blank filler panel
- Enhanced Conventional Gateway module (High Density (8 analog ports and 8 V.24 ports) or Low Density (four analog ports and four V.24 ports))
- Expansion module equipped with one of the following:
    - analog/V.24 interface kit (E&M daughterboard and two V.24 daughterboards)
    - FlexWAN daughterboards

NOTICE: One way to test that the hardware configurations match is to make sure that there is a connector on the replacement unit for each of the cables connected to the existing unit.

When and where to use: Use this procedure when replacing a router device in a non-hardended system.

Process:

1. Physically replace the router hardware. See Installing an S6000 Router in a Rack on page 31 or Replacing a Router – S2500 on page 102.
2. Execute the `Clear USM Cache` saved command in the VoyenceControl component of the Unified Network Configurator (UNC). `Clear USM Cache` is in the list of saved commands under **System** → **Motorola** → **SNMPv3**.

   For information about accessing and executing saved commands for a device, see the “Accessing and Executing Existing Saved Commands” section in the *Unified Network Configurator* manual.

   NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.
3. If you do not have the correct EOS version on Unified Network Configurator (UNC), load the EOS onto UNC. See Loading the EOS Image to the UNC Server on page 249.
4. On an S6000 Router, check the version of the firmware if performing a downgrade. If the version is 16.8.0.19 or higher for an NMR, additional steps are necessary. See Performing a Firmware Downgrade on page 250.
5. Extract the configuration files from the UNC. See Extracting Configuration Files from UNC on page 251.

6 Install an EOS image and manage SSH keys. See Installing an EOS Image and Managing SSH Keys on page 252.

7 Only if link encryption is required, add link encryption. See Adding Link Encryption on page 254.

8 Assign passwords. See Assigning Passwords on page 259.

9 Push the configuration to the router. See Pushing the Configuration to the Router on page 262.

10 Set up Information Assurance. See Setting up Information Assurance on page 263.

11 Test SNMPv3 Credentials. See Testing SNMPv3 Credentials on page 264.

12 Push the configurations from VoyenceControl to the secondary directory of the gateway. See Pushing Configurations to the Secondary Directory of a Router on page 264.

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

13 Pull the configuration to UNC. See Pulling the Configuration to Unified Network Configurator on page 265.

14 Delete the router from Unified Event Manager. See Deleting a Router from UEM on page 266.

15 Discover the router in Unified Event Manager. See Discovering a Router in UEM on page 266.

15.1.1

Loading the EOS Image to the UNC Server

When and where to use: This procedure is used by the Motorola Solutions Support Center (SSC) to load the EOS image (`boot.ppc`) on to the UNC server. Load the EOS image (`boot.ppc`) from the media device if you do not have the correct version of EOS on the UNC server. It is not necessary to perform this procedure if the correct version of the EOS already exists on the UNC server.

Procedure:

1 Perform the appropriate steps:

If…	Then…
You use PuTTY to log on to the UNC server,	perform the following tasks. a Using proper credentials for the UNC administrator, log on to UNC. b In the Host Name (or IP address) field, enter: ***`<username>`*** `@` ***`<IP address of the server>`*** **NOTICE:** Refer to the *Securing Protocols with SSH* manual for details. c At the prompt, enter: `su -` and the password for account with root privileges. d Press ENTER.
If you use VMware VSphere Client to access UNC,	perform the following tasks: a Start the **VMware VSphere Client** client from the **NM** client. b Select the following VMserver address: **10.*<z>*.233.122**, where ***<z>*** is the zone number. c Enter a username and password. d Select **UNC** from the list on the left pane.

If…	Then…
	e Select **Console**. **f** Enter a username and password.

2. At the root prompt, enter `admin_menu`

   The **Main Menu** displays.

3. Enter the number corresponding to the **Application Administration** option. Press ENTER.
4. In the **Application Administration** menu that displays, enter the number that corresponds to the **OS Images Administration** option. Press ENTER.
5. In the **OS Images Administration** menu that displays, enter the number that corresponds to the **Load new OS images** option. Press ENTER.

   Messages display, indicating that the OS image files referenced in the Voyence database are deleted and describing the two methods for loading an OS image. You are prompted to insert media now, if needed.

6. Insert the media device that contains the EOS `.tar` file to your PC's CD/DVD drive. Press ENTER.

   Messages appear with descriptions of the status of the image processing, followed by the **OS Images Administration** menu.

7. Enter the number corresponding to the **Eject CD/DVD** option. Press ENTER.

   The **CD/DVD ejected** message appears below the **OS Images Administration** menu.

8. Enter `q`. Press ENTER.

   The **User Quit** message appears, followed by the root prompt.

Postrequisites: Proceed to Extracting Configuration Files from UNC on page 251.

15.1.2 Performing a Firmware Downgrade

Starting with the 16.8.0.19 firmware, the digital signature algorithm is enhanced on the S6000 Router software. The enhancement prohibits the router from running an unsigned version of the EOS, or running a version of EOS that is signed with a prior pre-enhanced digital signature. If the EOS must be downgraded to a firmware version earlier than 16.8.0.19 but no older than 15.0.0.0, before applying the older firmware, a command must be run that allows the EOS and Boot Monitor to revert to using the older digital signature method for validating the firmware. After running the command, the downgrade can be executed.

If the router EOS version 16.8.0.19 or newer must be downgraded to a version older than 15.0.0.0, then a two-step process is required. Downgrade the EOS to 15.0.0.0 by performing the following procedure. Once the router is at 15.0.0.0, then downgrade to the older targeted EOS firmware version using normal procedures.

When and where to use: Use this procedure when downgrading the router.

Process:

1. To check the version of firmware on the router, enter: `sh ver`
2. Depending on the software version, choose one of the following:
   - Version 16.8.0.18 or lower means that the downgrade can use the older signature algorithm. Go to step 4.

- Version 16.8.0.19 or higher, go to step 3.

3 To change the SW Signing Algorithm, enter: `setd -sys ssa = SHA1withRSA1024`

NOTICE: If this command is not performed before loading the older firmware, an error message appears. After bootup, the router may not have firmware to run if the router is configured with only one boot source (a:/primary or a:/secondary) as the firmware location. The router can be recovered from the Boot Monitor by performing the following substep:

a Enter: `SA SHA1withRSA1024`

4 Depending on the final target version, choose one of the following:

- Version 15.0.0.0 or higher, can be directly downgraded from the current version. No further steps are necessary. Proceed as normal with the downgrade process.
- Version lower than 15.0.0.0, go to step 5.

NOTICE: If step 5 is not performed before loading the older firmware, an error message appears informing about the incorrect firmware authentication signature.

5 Downgrade the firmware to any version with the numbers from the pool: 16.7.X.X. After the router bootup with the new temporary firmware, enter: `SETDefault -SYS FIPS = OFF`

6 Proceed as normal with the downgrade process.

15.1.3

Extracting Configuration Files from UNC

Prerequisites: Obtain access to Unified Network Configurator (UNC).

Procedure:

1 On the PNM Client, open the VoyenceControl (10.0.0.2) application.

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

2 For the username and password, enter `Admin`.

3 Select **Tools** → **Networks Navigation**.

4 In the **Networks Navigation** window, select **Astro 25 Radio Network** → **Views**. Double-click **Motorola Network Resource**.

5 In the right pane, double-click the appropriate router.

The **Configs** window opens listing all the config files for the router, for example acl.cfg, boot.cfg, override.cfg, and staticRP.cfg.

6 In the left pane, double-click **A:/primary/acl.cfg** to open the acl.cfg file in the right pane.

NOTICE: If no acl.cfg file exists, for example no file is displayed in the right pane when you double-click the corresponding path in the left pane, continue with step 8.

7 Copy the acl.cfg file from the right pane, paste the file to a Notepad file. Save the file as acl.cfg.

8 Perform the following actions:

a Repeat steps 6 and 7 for the boot.cfg file:

- Double-click `A:/primary/boot.cfg` in step 6.
- Save the file as boot.cfg in step 7.

b Repeat steps 6 and 7 for the override.cfg file:

- Double-click `A:/primary/override.cfg` in step 6.
- Save the file as override.cfg in step 7.

c Repeat steps 6 and 7 for the staticRP.cfg file:

- Double-click `A:/primary/staticRP.cfg` in step 6.
- Save the file as staticRP.cfg in step 7.

d (GGSN routers only) Repeat steps 6 and 7 for the xgsn.cfg file:

- Double-click `A:/primary/xgsn.cfg` in step 6.
- Save the file as xgsn.cfg in step 7.

NOTICE: If the routers does not have a particular type of configuration file skip the step corresponding to that configuration file. For example, if the routers does not have an override.cfg configuration file, skip step b.

Postrequisites: Proceed to Installing an EOS Image and Managing SSH Keys on page 252.

15.1.4
Installing an EOS Image and Managing SSH Keys

Prerequisites: Ensure you have the required cabling and connectors.

When and where to use: Perform this procedure to install EOS, generate SSH keys on the device, and delete SSH keys on Unified Network Configurator (UNC).

Process:

1 Connect the new router to the laptop by using the console and Ethernet cables.

IMPORTANT: Do not connect the gateway to the WAN or LAN yet.

2 From the laptop, push the new EOS locally by using TFTP. See Pushing EOS Locally on page 252.

3 If SSH is enabled, perform the following actions:

a Generate SSH keys on the router by entering:

`GenSshKey` ***`<algorithm><bits>`***
Where RSA is the default ***`<algorithm>`*** and 2048 is the default ***`<bits>`*** value.

b Delete SSH keys on UNC. See Deleting SSH keys on UNC on page 253.

4 Continue with one of the following procedures:

- If you add link encryption, perform Adding Link Encryption on page 254.
- If you do not add link encryption, perform Assigning Passwords on page 259.

15.1.4.1
Pushing EOS Locally

Push new EOS locally from a laptop by using TFTP.

Procedure:

1 Log on to the router by using the console connection. Enter the username (root) and appropriate password (usually no password on a new gateway).

2 Point the TFTP server to the boot.ppc file.

3 Assign an IP address to the laptop with the appropriate subnet mask.

For example, assign 10.0.0.1 with 255.255.255.0.

NOTICE: This IP address has to be in the same subnet as the router interface that is connected to the laptop Ethernet card.

4 Connect the laptop Ethernet card to port 1 of the device (!1) by using a crossover cable.

5 On the router (with the 10.0.0.2 IP address in this example), perform the following actions:

   a Enter: `setd !1 -ip netaddr= 10.0.0.2 255.255.255.0`

   b Enter: `setd !1 -po cont=e`

   c Enter: `setd !1 -pa cont=e`

6 To check if Port 1 status is up, enter: `show -ip neta`

7 Ping the laptop IP address to check connectivity.

8 Enter: `copy 10.0.0.1:/boot.ppc a:/primary/boot.ppc`

NOTICE: The boot.ppc file is copied from the TFTP directory into the router primary directory. The file transfer takes about 1 to 3 minutes.

9 Reboot the router .

10 After the reboot, verify EOS by entering: `show -sys soi a:/primary/boot.ppc`

This command displays the EOS software package and version number for the specified boot file in the gateway primary directory. Verify that the correct package and version are listed.

Postrequisites: Return to step 3 in Installing an EOS Image and Managing SSH Keys on page 252.

15.1.4.2
Deleting SSH keys on UNC

Procedure:

1 Access the Unified Network Configurator (UNC) server by using its IP address.

2 In the login prompt that displays, enter the UNC administrator account credentials.

3 In the **UNC Administration Menu** that appears, perform the following actions:

   a Enter the corresponding number for **OS Administration**. Press Enter.

   b Enter the corresponding number for **Security Provisioning**. Press Enter.

   c Enter the corresponding number for **Delete Device's Public SSH Key**. Press Enter.

4 Enter the IP address for the device.

The key is deleted.

5 Right-click the device in the VoyenceControl component of the UNC, select **Quick Commands Test Credentials** to establish an SSH connection.

The connection automatically adds the device's SSH host key to the UNC known hosts list.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.
Before you use Test Credentials, ensure that SSH/SCP are selected as the protocols that UNC will use for communication with the device.

Postrequisites: Return to step 4 in Installing an EOS Image and Managing SSH Keys on page 252.

15.1.5

Adding Link Encryption

Process:

1 Perform one of the following actions:

- To add link encryption on the site router, perform Adding Link Encryption on Site Router on page 254.
- To add link encryption on the core or exit router, perform Adding Link Encryption on Zone Router on page 257.

NOTICE: This procedure does not apply to gateway or GGSN routers.

15.1.5.1

Adding Link Encryption on Site Router

Prerequisites: Obtain the location of the required pre-shared keys from your system administrator. The ***<pre-shared key>*** value is the customer-specific secret passphrase.

When and where to use:

NOTICE: Perform this procedure only if Link Encryption is required.

IMPORTANT: This procedure adds crypto keys on the site router. The keys **must** match the ones on the core routers or gateways for each site link.

Procedure:

1 Log on to the appropriate site router by using the console connection and a null modem serial cable. Enter the username (root) and the appropriate password (usually no password on a new device).

2 Connect a crossover Ethernet cable between the laptop and the router.

3 Assign an IP address to the laptop with the appropriate subnet mask.

For example, assign 10.0.0.1 with 255.255.255.0. This IP address has to be in the same subnet as the router's interface that will be connected to the laptop's Ethernet card.

4 On the router (in this example the IP address 10.0.0.2.), enter:

```
setd !1 -ip netaddr= 10.0.0.2 255.255.255.0

setd !1 -po cont=e

setd !1 -pa cont=e
```

5 Add crypto keys for the associated core routers or gateways:

If…	Then…
If you add crypto keys for IPv4 links,	perform the following actions: **a** Enter: `add -crypto fipspreshrdkey` ***<SysIP_Core1>*** "***<pre-shared key>***" "***<pre-shared key>***" where:

If…	Then…
	<SysIP_Core1> is the system IP address of core router 1 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks) **b** Enter: `add -crypto fipspreshrdkey` ***<SysIP_Core2> “<pre-shared key>” “<pre-shared key>”*** where: ***<SysIP_Core2>*** is the system IP address of core router 2 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks)
If you add crypto keys for IPv6 links,	perform the following actions: **a** Enter: `add -crypto fipspreshrdkey ikev2` ***<Core1_IPv6_backhaul address> “<pre-shared key>” “<pre-shared key>”*** where: ***<Core1_IPv6_backhaul address>*** is the IPv6 backhaul address of core router 1 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks) **b** Enter: `add -crypto fipspreshrdkey ikev2` ***<Core2_IPv6_backhaul address> “<pre-shared key>” “<pre-shared key>”*** where: ***<Core2_IPv6_backhaul address>*** is the IPv6 backhaul address of core router 2 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks)
If you add crypto keys for IPv4 links and for architectures where the subsites are connected to the Prime Site through a backhaul switch,	perform the following actions: **a** Enter: `add –crypto fipspreshrdkey` ***<SysIP_AccessRouter1> “<pre-shared key>” “<pre-shared key>”*** where: ***<SysIP_AccessRouter1>*** is the system IP address of access router 1 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks) **b** Enter: `add –crypto fipspreshrdkey` ***<SysIP_AccessRouter2> “<pre-shared key>” “<pre-shared key>”*** where: ***<SysIP_AccessRouter2>*** is the system IP address of access router 2

If…	Then…
	<pre-shared key> is the pre-shared key (which must be enclosed in quotation marks)
If you add crypto keys for IPv6 links and for architectures where the subsites are connected to the Prime Site through a backhaul switch,	perform the following actions: **a** Enter: `add -crypto fipspreshrdkey ikev2` ***<AccessRouter1_IPv6_backhaul address>*** "***<pre-shared key>***" "***<pre-shared key>***" where: ***<AccessRouter1_IPv6_backhaul address>*** is the IPv6 backhaul address of access router 1 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks) **b** Enter: `add -crypto fipspreshrdkey ikev2` ***<AccessRouter2_IPv6_backhaul address>*** "***<pre-shared key>***" "***<pre-shared key>***" where: ***<AccessRouter2_IPv6_backhaul address>*** is the IPv6 backhaul address of access router 2 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks)
If you add crypto keys for systems with the Dynamic System Resilience feature implemented,	perform the following actions: **a** Enter: `add -crypto fipspreshrdkey ikev2` ***<Core9_IPv6_backhaul address>*** "***<pre-shared key>***" "***<pre-shared key>***" where: ***<Core9_IPv6_backhaul address>*** is the IPv6 backhaul address of core router 9 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks) **b** Enter: `add -crypto fipspreshrdkey ikev2` ***<Core10_IPv6_backhaul address>*** "***<pre-shared key>***" "***<pre-shared key>***" where: ***<Core10_IPv6_backhaul address>*** is the IPv6 backhaul address of core router 10 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks)

6. Enter `sh -crypto fipspreshrdkey` on the site router and on the router on the other end of the site link. Verify that the key strings match.
7. Connect the LAN cable to the new router and connect it to the switch on the other end.
8. Connect the T1 cable or the Ethernet WAN cable to the appropriate ports.

9 Observe that both the link and activity LEDs for the T1 or Ethernet WAN port illuminate (the site transitions to site trunking).

10 To monitor link status, open a command prompt and run a continuous ping to the master site.

> ⚠ **CAUTION:** This procedure adds crypto keys on core and exit routers. The keys on the core routers must match the keys on the site router(s) on the other end of the site link(s). The keys on the exit routers must match the keys on the exit routers in the connecting zone.

11 When instructed by the master site, enter:

```
setd !v<port#> –crypto cont = e
```

on the site router, where ***<port#>*** is the port on which you activate link encryption.

12 If the link does not come back up, enter:

```
setd !v<port#> –crypto cont = d
```

on the site router and on the core router or gateway on the other end of the site link, to disable the encryption on both ends.

13 Verify that the FIPS pre-shared keys match. Type `sh -crypto fipspreshrdkey` on both devices and compare the results.

15.1.5.2

Adding Link Encryption on Zone Router

Prerequisites: Obtain the location of the required pre-shared keys from your system administrator. The ***<pre-shared key>*** value is the customer-specific secret passphrase.

When and where to use: Perform this procedure only if link encryption is required; otherwise proceed to Assigning Passwords on page 259.

> **IMPORTANT:** This procedure adds crypto keys on core and exit routers, or core/exit routers. The keys on the core routers or core/exit routers**must** match the keys on the site router(s) on the other end of the site link(s). The keys on the exit routers or core/exit routers must match the keys on the exit routers or core/exit routers in the connecting zone.

Procedure:

1 Log on to the appropriate core or core/exit router by using the console connection and a null modem serial cable. Enter the username (root) and the appropriate password (usually no password on a new device).

2 Connect a crossover Ethernet cable between the laptop and the router.

3 Assign an IP address (for example, 10.0.0.1) to the laptop with the appropriate subnet mask (for example, 255.255.255.0). This IP address has to be in the same subnet as the IP address of the router interface that is connected to the laptop’s Ethernet card

4 On the router (with IP address 10.0.0.2 in this example), perform the following actions:

  a Enter: `setd !1 -ip netadr = 10.0.0.2 255.255.255.0`

  b Enter:

```
setd !1 -po cont = e
```

```
setd !1 -pa cont = e
```

5 To add crypto keys on the core or core/exitrouter for the associated site router(s) (for site routers 1 and 2 in the following examples), perform the following actions:

- For IPv4 links, perform the following actions:
  - For a single-site link, on the core or core/exit router pair enter:

    `add -crypto fipspreshrdkey` ***<SysIP_Site_Router1>*** “***<pre-shared key>***” “***<pre-shared key>***”

    - For a dual-site link, on the core or core/exit router pair enter:
      `add -crypto fipspreshrdkey` ***<SysIP_Site_Router1>*** “***<pre-shared key>***” “***<pre-shared key>***”
      `add -crypto fipspreshrdkey` ***<SysIP_Site_Router2>*** “***<pre-shared key>***” “***<pre-shared key>***”

  Where ***<SysIP_Site_Router1>*** is the system IP address of site router 1, ***<SysIP_Site_Router2>*** is the system IP address of site router 2, and ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks).

- For IPv6 links, perform the following actions:
    - For a single-site link, on the core or core/exit router pair enter:
      `add -crypto fipspreshrdkey ikev2` ***<Site_Router1_IPv6_backhaul_address>*** “***<pre-shared key>***” “***<pre-shared key>***”
    - For a dual-site link, on the core or core/exit router pair enter:
      `add -crypto fipspreshrdkey ikev2` ***<Site_Router1_IPv6_backhaul_address>*** “***<pre-shared key>***” “***<pre-shared key>***”
      `add -crypto fipspreshrdkey ikev2` ***<Site_Router2_IPv6_backhaul_address>*** “***<pre-shared key>***” “***<pre-shared key>***”

  Where ***<Site_Router1_IPv6_backhaul_address>*** is the IPv6 backhaul IP address of site router 1, ***<Site_Router2_IPv6_backhaul_address>*** is the IPv6 backhaul IP address of site router 2, and ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks).

  NOTICE: The site router may be at an RF site, Prime Site, NM Dispatch site, or conventional subsystem site.

6 To add crypto keys on the exit or core/exit router pair for the exit or core/exit routers in the connecting zone (for exit or core/exit router 1 and site router 1 and exit or core/exit router 2 in the following examples), perform the following actions:

  IMPORTANT: They keys must match the keys on the exit or core/exit router in the connecting zone.

- For IPv4 links, perform the following actions on the exit or core/exit router pair:
    - Enter:
      `add -crypto fipspreshrdkey` ***<SysIP_Exit_Router1>*** “***<pre-shared key>***” “***<pre-shared key>***”
    - Enter:
      `add -crypto fipspreshrdkey` ***<SysIP_Exit_Router2>*** “***<pre-shared key>***” “***<pre-shared key>***”

  Where ***<SysIP_Exit_Router1>*** and ***<SysIP_Exit_Router2>*** are the system IP addresses of exit or core/exit routers in the other zone to which these exit or core/exit routers connect, and ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks).

- For IPv6 links, perform the following actions:
    - Enter:
      `add -crypto fipspreshrdkey ikev2` ***<Exit_Router1_IPv6_backhaul address>*** “***<pre-shared key>***” “***<pre-shared key>***”

- Enter:

  ```
  add -crypto fipspreshrdkey ikev2 <Exit_Router2_IPv6_backhaul
  address> “<pre-shared key>” “<pre-shared key>”
  ```

  Where ***<Exit_Router1_IPv6_backhaul address>*** and ***<Exit_Router2_IPv6_backhaul address>*** are the IPv6 backhaul addresses of the exit or core/exit routers in the other zone to which these exit or core/exit routers connect, and ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks).

7 Enter the following command on the routers at both ends of the encrypted link (the core or core/exit router and the site router(s) at the other end of the site link or the exit or core/exit router and the exit or core/exit router in the connecting zone):

```
sh -crypto fipspreshrdkey
```

Verify that the key strings match.

8 Connect the LAN cable to the new router and connect it to the switch on the other end.

9 Connect the T1 cable or the Ethernet WAN cable to the appropriate ports.

10 To monitor link status, open a command prompt and run a continuous ping to the remote site.

> **CAUTION:** Do not press ENTER after the following steps until you contact the remote site. This is a coordinated effort between personnel at the master site and the remote sites.

11 As coordinated with the remote site, enter:

```
setd !v<port#> —crypto cont = e
```

on each core or exit, or core/exit router, where ***<port#>*** is the port on which you activate link encryption.

12 If the link does not come back up, enter:

```
setd !v<port#> —crypto cont = d
```

on the core or core/exit router and on the site router at the other end of the site link or on the exit or core/exit router and the exit or core/exit router in the other zone to which it is connected to disable encryption, where ***<port#>*** is the port on which you disable link encryption. Then, verify that the FIPS pre-shared keys match by comparing the results after you enter: `sh –crypto fipspreshrdkey` on the routers at both ends of the link.

15.1.6
Assigning Passwords

Procedure:

1 If RADIUS is not enabled, go to step 2. If RADIUS is enabled, add a RADIUS secret key:

   a Log on to the router by using the console connection. Enter the username (root) and the appropriate password (usually no password on a new router).

   b Enter: `setd –ac secret = “<secret>”`

   Where ***<secret>*** is the RADIUS secret (up to 32 characters).

   The RADIUS secret which must be enclosed in quotation marks and must match the RADIUS secret on the RADIUS server.

   c To set the security server type to RADIUS, enter `setd -ras st=radius`.

2 Assign a root password to the router.

   a Enter: `Setd NMpassword = “<old_password>” “<new_password>” “<new_password>”`

Where ***<old_password>*** is the existing password (generally "" (blank string) on a new router) and ***<new_password>*** is the new password. The old and new passwords must be enclosed in quotation marks.

NOTICE: ***<new password>*** is case-sensitive and must be at least 7 but no more than 15 characters in length. Valid characters are limited to ASCII codes 32 through 126.
The string of six asterisks (******) is not allowed as a Network Manager password. This string is reserved for use as a nonoperational value when passwords are captured using the ASCII capture feature.

3 If PIM authentication is enabled, add the keys, and transition the device from **Transit** to **Secure** state. See Manually Enabling PIM Authentication on page 260.

NOTICE: Ensure that the right keys are used.

4 If OSPF authentication is enabled, refer to the “Enabling Transport Devices for OSPF MD5 Authentication for CNI Transport Devices” section in the *Link Encryption and Authentication* manual for instructions on how to manually configure the OSPF authentication features.

5 If BGP authentication is enabled, refer to the “Enabling Transport Devices for BGP MD5 Authentication on CNI Transport Devices” section in the *Link Encryption and Authentication* manual for instructions on how to manually configure the BGP authentication features.

6 Reboot the router once.

7 Continue with Pushing the Configuration to the Router on page 262.

15.1.6.1
Manually Enabling PIM Authentication

Prerequisites: This procedure assumes that a global security association has been configured and enabled for all PIM-enabled devices across the domain. Before beginning this procedure, obtain the policy name for the global security association used for PIM authentication as well as the authentication key used for all PIM-enabled devices across the domain.

When and where to use: Perform this procedure to configure and manually enable PIM authentication on all PIM-enabled devices across the domain.

Procedure:

1 Define a keyset for PIM authentication on the device by entering the following command:

```
ADD -crypto ManKeySet <keyset_name> AuthKey “<auth-key>” “<auth-key>”
```

Where ***<keyset_name>*** is a unique 1-15 character name and ***<auth_key>*** is the authentication key (enclosed in quotation marks). You can include standard alphanumeric characters and special characters (other than quotation marks) in the authentication key.

Step example: For example, to configure keyset “mks1” with authentication key “secret”, enter:

```
ADD -crypto ManKeySet mks1 AuthKey “secret” “secret”
```

IMPORTANT: The ***<keyset_name>*** must match the ***<keyset_name>*** that is configured on the device’s PIM authentication peers. In addition, the authentication key should be the same for all PIM-enabled routers and gateways across the domain. To view the authentication key configured on a PIM authentication peer, enter the following command on the peer:

```
SHow -crypto ManKeySet
```

2 Create a global security association (SA) on the device by entering the following command:

```
ADD -crypto GblManKeyInfo <policy_name><keyset_name> SpiAh
<spi_in><spi_out>
```

Where ***<policy_name>*** is the policy name defined for the global manual security policy used for PIM authentication; ***<keyset_name>*** is the keyset name defined with the `ManKeySet` parameter; and ***<spi_in>*** and ***<spi_out>*** are the incoming and outgoing authentication SPI values (256-512).

NOTICE: ***<spi_in>*** and ***<spi_out>*** must be the same value.

Step example: For example to create a global manual security association that binds policy “pim1” with keyset “mks1” and an incoming and outgoing authentication SPI value of 300, enter:

```
ADD -crypto GblManKeyInfo pim1 mks1 SpiAh 300 300
```

3 Specify that the global SA you created in step 2 is the transmit SA (the SA which will be used to authenticate outgoing packets using the specified SPI value) by entering the following command:

`ADD -crypto GblManXmitSA` ***<policy_name><spi_out>***

Where ***<policy_name>*** is the policy name defined for the global manual security policy used for PIM authentication and ***<spi_out>*** is the outgoing authentication SPI value.

Step example: For example to specify policy “pim1” (with outgoing authentication SPI value 300) as the transmit SA, enter:

```
ADD -crypto GblManXmitSA pim1 300
```

NOTICE: If you do not specify an active transmit SA, the device uses the SA with the lowest ***<spi_out>*** value as the transmit SA.

4 Set the PIM authentication state to “Transit” on the device you are configuring for PIM authentication, as well as its PIM authentication peers, by entering:

`ADD -crypto GblManPolState` ***<policy_name>*** `Transit`

Where ***<policy_name>*** is the policy name defined for the global manual security policy used for PIM authentication.

Step example: For example to set the PIM authentication state for policy “pim1” to “Transit”, enter:

```
ADD -crypto GblManPolState pim1 Transit
```

IMPORTANT: Put all PIM-enabled routers and gateways configured for PIM authentication in “Transit” state at the same time to avoid losing communication between the PIM devices. If some devices are placed in “Transit” state and others are left in “Clear” state, a communication failure will occur.

NOTICE: The device remains in PIM authentication “Transit” state until you explicitly move it to any other state using the `ADD -crypto GblManPolState` command.

5 Enter the following command to display the PIM authentication state and verify that it is set to “Transit”:

`SHow -crypto GblManPolState` ***<policy_name>***

Where ***<policy_name>*** is the policy name defined for the global manual security policy used for PIM authentication.

Step example: For example to display the PIM authentication state for policy “pim1”, enter:

```
SHow -crypto GblManPolState pim1
```

6 Reboot the device and connect it to the LAN.

7 Display the PIM authentication status on the device you are configuring for PIM authentication, as well its PIM authentication peers, by entering:

```
SHow -crypto ManPeerReport
```

IMPORTANT: Verify that the **Authentication Result** is PASS for all peers. If the **Authentication Result** column lists FAIL for any peer, verify that the SAs on that peer are configured correctly.

8. Set the PIM authentication state to "Secure" on the device you are configuring for PIM authentication, as well as its PIM authentication peers, by entering:

   `ADD -crypto GblManPolState <policy_name> Secure`

   Where ***<policy_name>*** is the policy name defined for the global manual security policy used for PIM authentication.

   Step example: For example to set the PIM authentication state for policy "pim1" to "Secure", enter:

   `ADD -crypto GblManPolState pim1 Secure`

   IMPORTANT: Put all PIM-enabled routers and gateways configured for PIM authentication in "Secure" state at the same time to avoid losing communication between the PIM devices. If some devices are placed in "Secure" state and others are left in "Transit" state, a communication failure will occur.

9. Enter the following command to display the PIM authentication state and verify that it is set to "Secure":

   `SHow -crypto GblManPolState <policy_name>`

   Where ***<policy_name>*** is the policy name defined for the global manual security policy used for PIM authentication.

   Step example: For example to display the PIM authentication state for policy "pim1", enter:

   `SHow -crypto GblManPolState pim1`

15.1.7

Pushing the Configuration to the Router

Prerequisites: Install Trivial File Transfer Protocol (TFTP) server software.

When and where to use: Use this procedure to copy the configuration files from the TFTP directory into the device's primary directory.

Procedure:

1. To log on, point the TFTP server to the appropriate location, assign an IP address to the laptop, and connect to the Ethernet card:
   - **a** Log in to the router (Console connection) using the username (root) and the appropriate password (usually no password on a new router).
   - **b** Point the TFTP server on the laptop to the boot.cfg file and other cfg files (acl.cfg, staticRP, override.cfg, if applicable).
   - **c** Assign an IP address (for example, 10.0.0.1) to the laptop with the appropriate subnet mask (for example, 255.255.255.0). This IP address has to be in the same subnet as the IP address of the gateway interface that is connected to the laptop's Ethernet card.
   - **d** Connect the laptop's Ethernet card to port 1 of the router (!1) using a crossover cable.
2. Perform the following actions on the router (this example uses IP address 10.0.0.2):
   - **a** Enter: `setd !1 -ip netaddr= 10.0.0.2 255.255.255.0`
   - **b** Enter: `setd !1 -po cont=e`
   - **c** Enter: `setd !1 -pa cont=e`
3. To check if Port 1 status is Up, enter: `show -ip neta`
4. Ping the laptop IP address to check connectivity.

5. To copy the configuration files from the TFTP directory into the router's primary directory, perform the following actions:

   NOTICE: If the router does not have a particular type of configuration file skip the command line corresponding to that configuration file. For example, if the router does not have an override.cfg configuration file, skip the `copy 10.0.0.1:/override.cfg a:/primary/override.cfg` command.

   a Enter: `copy 10.0.0.1:/boot.cfg a:/primary/boot.cfg`

   b Enter: `copy 10.0.0.1:/acl.cfg a:/primary/acl.cfg`

   c If applicable, enter: `copy 10.0.0.1:/override.cfg a:/primary/override.cfg`

   d Enter: `copy 10.0.0.1:/staticRP.cfg a:/primary/staticRP.cfg`

   e For a GGSN router only, enter: `copy 10.0.0.1:/xgsn.cfg a:/primary/xgsn.cfg`

6. To view the boot.cfg file and ensure it matches what was deployed, perform the following actions:

   a Enter: `cd`

   b Enter: `cat boot.cfg`

7. For all other configuration files loaded on the gateway (acl.cfg, override.cfg, staticRP.cfg), repeat step 6.

15.1.8

Setting up Information Assurance

Prerequisites: Contact your system administrator for IP addresses.

When and where to use: Perform this procedure to set up Information Assurance (IA) on the devices.

Procedure:

1. When IA is in use, enable SNMPv3 auth/priv with correct passphrases. Refer to the "Configuring MNR Routers and GGM 8000 Gateways for SNMPv3" section in the *SNMPv3* manual.
2. Reboot the router.
3. Disable MAC Port Lockdown:

   a Log on to the switch by using the console connection. Enter the username and the appropriate password.

   b Enter the following commands:

   ```
   config
   no port-security <port#>
   ```

   Where ***<port#>*** is the switch port on which you are disabling MAC Port Lockdown.

4. Connect the new router (port 1) to port 1 of the switch for the LAN connection.
5. Turn on the router.

   The LAN and WAN link come up.

6. Connect to the site LAN switch ***<port#>***, where ***<port#>*** is the switch port on which you are enabling MAC Port Lockdown. Perform the following actions:

   a Enter: `interface <port#> enable`

   b Enter: `port-security <port#> clear-intrusion-flag`

   c Enter: `port-security <port#> learn-mode static address-limit 31`

NOTICE: This command is given to learn the MAC addresses on the particular port specified. The switch does not learn the MAC address of the connected device dynamically. You may have to ping the device for the switch to learn its MAC address. Contact your system administrator for the IP addresses.

7 In case of dual devices, reboot the primary device. This will cause the second device to take over through the VRRP session. This will also cause the VRRP MAC to appear on the switch port enabled for learn mode.

8 Enter `show port-security` ***`<port#>`***

The MAC addresses associated with the port appear. This number of MAC addresses should be used for ***`<numberMacAllowed>`***.

9 To lock the port, perform the following actions:

a Enter:

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

b Enter: `show interfaces brief`

NOTICE: This command is used to show the status of the port to which MAC Port Lockdown is applied.

15.1.9

Testing SNMPv3 Credentials

Procedure:

1 Log on to VoyenceControl.

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

2 From **Networks** in the navigation pane, select **Astro 25 Radio Network** → **Views**.

3 In the navigation pane, double-click **Devices**.

4 Hold down the CTRL key. Click the device for which you want to check credentials.

5 Right-click one of the selected devices.

6 Select **Quick Commands** → **Test Credentials**.

NOTICE: Troubleshoot if the credentials are not correct.

15.1.10

Pushing Configurations to the Secondary Directory of a Router

When and where to use: Perform this procedure to push configurations from VoyenceControl to the router's secondary directory.

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

Procedure:

1 Log on to the VoyenceControl application.

2 In the navigation pane, select **Networks** → **Astro 25 Radio Network**.

3 Double-click **Motorola Network Resource**.

4. In the navigation pane, select **Workspaces** and double-click **TNCT *`<Date>`***.

   `<Date>` is the date associated with the appropriate TNCT configuration files.

5. Start the push for the configuration files. See Starting a Configuration File Push on page 265.

15.1.10.1

Starting a Configuration File Push

Procedure:

1. In the **Selected Device** list, select the routers to which you want to load the configuration files.
2. Right-click the selected routers. Select **Schedule** → **Select All** → **Schedule**.
3. In the **Job Name** field, type a name for the job.
4. Select the **Tasks** tab.
5. Click the router in the **Post Operation** column.
6. Click **OK**.
7. Click **Approve & Submit**.
8. Reboot the router:

   a. Return to the terminal program.

   b. At the `EnterpriseOS#` prompt, enter: `rb` (ReBoot). Press Enter.

   The router reboots and processes the configuration files. Once complete, `System Initialized and Running` is displayed.

9. Press F7.

   The Schedule Manager dialog box appears. The configuration push to the device takes approximately 1 minute to complete. The state for the device appears as **Completed** and a green dot appears next to the device when the push is complete. A red dot appears next to the device if the push fails and the state shows **Failed**.

15.1.11

Pulling the Configuration to Unified Network Configurator

When and where to use: Pull the configuration from the router to Unified Network Configurator (UNC).

Procedure:

1. Log on to the VoyenceControl application.

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

2. In the navigation pane, select **Networks** → **Astro 25 Radio Network**.
3. Double-click **Devices**.
4. Navigate to the device. Right-click the name of the view from which you want to pull device configurations.
5. Select **Pull** → **Pull Config**.

   The configuration for the selected device is pulled back into UNC and the device and UNC are now synchronized.

6. After the pull is complete, verify the configuration.

15.1.12
Deleting a Router from UEM

Procedure:

1 Log on to Unified Event Manager (UEM).

2 From the **Network Database** view, select a row.

3 Right-click selected row and select **Delete Object and Traces**.

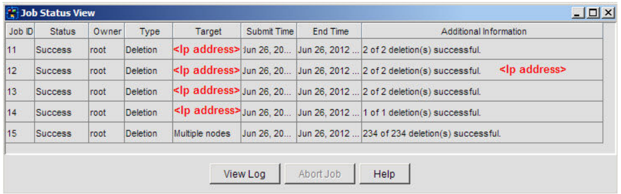
4 In the confirmation dialog box, click **Yes**.

5 In the **Deletion Status** dialog box, click **View Job Status**.

A separate job is initiated for each deletion request. The status of the request appears in the **Job Status View** window.

6 In the **Job Status View** window, verify the deletion status.

Figure 80: Job Status View for Deletion Jobs Window



Job ID	Status	Owner	Type	Target	Submit Time	End Time	Additional Information
11	Success	root	Deletion	<Ip address>	Jun 26, 20...	Jun 26, 2012 ...	2 of 2 deletion(s) successful.
12	Success	root	Deletion	<Ip address>	Jun 26, 20...	Jun 26, 2012 ...	2 of 2 deletion(s) successful. <Ip address>
13	Success	root	Deletion	<Ip address>	Jun 26, 20...	Jun 26, 2012 ...	2 of 2 deletion(s) successful.
14	Success	root	Deletion	<Ip address>	Jun 26, 20...	Jun 26, 2012 ...	1 of 1 deletion(s) successful.
15	Success	root	Deletion	Multiple nodes	Jun 26, 20...	Jun 26, 2012 ...	234 of 234 deletion(s) successful.

If the job status is **Success** or **Completed** the device or node and the alarms associated with it are also deleted. Events are not deleted, as events are part of the history and they are deleted only when the database is reinitialized.

7 If the **Warning Discovery in progress** dialog box appears, to the view active jobs that are related to the object being deleted, click **Open Job View**.

NOTICE: Once a device is deleted, you cannot restore its alarms.

Job View with the first job highlighted appears.

15.1.13
Discovering a Router in UEM

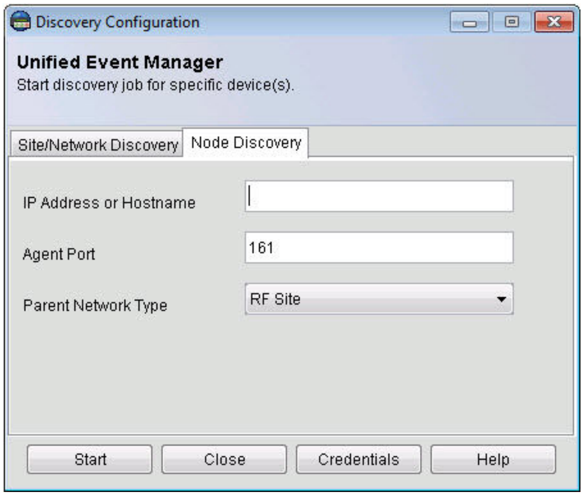
Procedure:

1 Log on to Unified Event Manager (UEM).

2 From the menu, select **Tools** → **Discovery**.

3 In the **Discovery Configuration** window, click the **Node Discovery** tab.

Figure 81: Discovery Configuration – Node Discovery



Unified Event Manager
Start discovery job for specific device(s).

IP Address or Hostname

Agent Port: 161

Parent Network Type: RF Site

4 In the **Node Discovery** tab, provide discovery credentials:

   a In the **IP Address or Hostname** field, enter an IP address or hostname of the device you want to discover.

   b In the **Agent Port** field, enter an SNMP agent port.

   You can leave the default value unchanged as it applies to most of devices.

   c From the **Parent Network Type** list, select the parent network type. Click **Start**.

   NOTICE: The Parent Network Type value is used to create the appropriate Network managed resource. It applies when the IP address being discovered is the first node added to UEM in this subnet. The network type that the device belongs to can be different from the physical location of the device.
   For example, choose **RF Site** when discovering a device at a site that is physically located at the Primary Zone Core.

5 In the **IP Address or Hostname** field, enter an IP address or hostname of the device you want to discover.

6 In the **Agent Port** field, enter an SNMP agent port.

You can leave the default value unchanged as it applies to most devices.

7 Click **Start**.

8 In the **Node Discovery Status** window, click **View Job Status**.

For each discovery request, a separate job is initiated. You can view jobs statuses in the **Job Status View** window.

In the**Job Status View** window, the status of the discovery is displayed. If the discovery is based on hostname, the **TARGET** column shows the hostname with the IP address appended.