System Release 7.17
ASTRO® 25
INTEGRATED VOICE AND DATA

Flexible Site and InterZone Links

NOVEMBER 2016

MN003276A01-A

Copyrights

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

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.

This page intentionally left blank.

Contact Us

Motorola Solutions Support Center

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

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

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

North America Parts Organization

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

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

Comments

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

Provide the following information when reporting a documentation error:

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

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

This page intentionally left blank.

Document History

Version	Description	Date
MN003276A01-A	Original release of the *Flexible Site and Inter-Zone Links* manual.	November 2016

This page intentionally left blank.

Contents

This page intentionally left blank.

List of Figures

This page intentionally left blank.

List of Tables

This page intentionally left blank.

List of Processes

This page intentionally left blank.

List of Procedures

This page intentionally left blank.

About Flexible Site and InterZone Links

This document describes the Flexible Site and InterZone Links feature (also referred to as Ethernet links) that provides alternate connectivity options for linking zones and sites in a Motorola Solutions ASTRO® 25 system.

What is Covered In This Manual?

This manual contains the following chapters:

- Description on page 25, introduces the Flexible Site and InterZone Links feature.
- Theory of Operations on page 31, describes technical concepts relating to the Flexible Site and InterZone Links feature.
- Installation and Configuration on page 43, covers the installation and configuration of system components to implement the Flexible Site and InterZone Links feature.
- Optimization on page 51, describes the optimization of the Flexible Site and InterZone Links feature.
- Operation on page 53, provides information relevant to the operation of the Flexible Site and InterZone Links feature.
- Troubleshooting on page 55, provides tools and techniques to troubleshoot the Flexible Site and InterZone Links feature.
- FRU/FRE Information on page 61, lists Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs), and includes replacement procedures applicable to the Flexible Site and InterZone Links feature.
- Ethernet Site Links – Expansion on page 63, contains the activities required to perform the expansion of Ethernet Site Links.

Helpful Background Information

The Motorola Solutions technical training team offers various courses designed to assist in learning about the system. For a complete list of available courses and schedules, go to http://www.motorolasolutions.com/training to view the current course offerings and technology paths.

Related Information

See the following documents for associated information about the radio system.

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

Table continued…

Related Information	Purpose
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.
L and M Core Conventional Architectures Engineer Guide	Describes the centralized conventional architectures and distributed conventional architecture supported by L or M core ASTRO® 25 systems.
Dynamic System Resilience Feature Guide	Provides the information necessary to understand, operate, maintain, and troubleshoot the Dynamic System Resilience (DSR) feature that adds a geographically separate backup zone core to an existing zone core to protect against catastrophic zone core failures.
Link Encryption and Authentication	Provides information on the implementation and management of router encryption and authentication for ASTRO® 25 systems, including details about encryption modules and configuration sequences for minimizing downtime, to support encrypted links between routers that traverse an untrusted network. Router authentication enables peer routers to use pre-shared keys to authenticate messages received from various routing protocols.
MLC 8000 Configuration Tool User Guide	Provides information about an application used for configuration, analog voting display, and analog voting control for the MLC 8000 device, functioning as an analog conventional comparator for analog IP-based simulcast and non-simulcast voting, and as a subsite link converter for conventional analog, digital and mixed mode channels.
Securing Protocols with SSH	Provides information on the implementation and management of the Secure SHell (SSH) protocol for secure transmission of data between devices in ASTRO® 25 systems, including configuration sequences that minimize downtime when adding this feature to a system that is already in operation.
Service Access Architecture	Provides information on the implementation of a secure connection between a service laptop and the ASTRO® 25 system, including examples of access scenarios.
GGM 8000 System Gateway	Provides information relating to the installation, configuration and management of the GGM 8000 Gateway as used at in various network locations.
S6000 and S2500 System Routers	Provides information relating to the installation, configuration and management of the S6000 and S2500 routers as used in various network locations.
System LAN Switches	Provides use of Hewlett-Packard (HP) switches in ASTRO® 25 systems, including LAN switches and backhaul switches. In addition to common procedures for installation, configuration, operation, and troubleshooting of the switches, this manual provides information for specific ASTRO® 25 system sites and features that HP switches can support.
Terminal Servers LX Series	Covers installation, configuration and management of the In-Reach® 8000 (LX-4000S) series Terminal Server which supports a network management connection to servers and network transport equipment in the zone.

Table continued…

Related Information	Purpose
Trunked IP Simulcast Subsystem Prime Site	Covers the installation, configuration and management of an ASTRO® 25 trunked system IP simulcast prime site employing the GCP 8000 Site Controller and GCM 8000 Comparator.
Unified Network Configurator	Covers the use of Unified Network Configurator (UNC), a sophisticated network configuration tool that provides controlled and validated configuration management for system devices including routers, LAN switches, site controllers and base radios, and is used to set up sites for the ASTRO® 25 system. UNC has two components: Voyence Control and Unified Network Configurator Wizards (UNCW).
Unified Event Manager	Covers the use of Unified Event Manager (UEM) provides reliable fault management services for devices in ASTRO® 25 systems.
Zone Core Protection Infrastructure	Provides information relating to the implementation and management of the Zone Core Protection (ZCP) feature available for ASTRO® 25 systems. ZCP is an optional configuration of hardware and software components for supporting network security at the zone core (master site). ZCP-specific components covered in this manual include ZCP firewalls, Mediation LAN switches, and a Motorola Solutions-supplied intrusion detection solution.

This page intentionally left blank.

Chapter 1

Description

This chapter provides a high-level description of the Flexible Site and InterZone Links feature and the function it serves on your system.

1.1 Introduction

Motorola Solutions ASTRO® 25 system site and InterZone links traditionally use dedicated T1/E1 links for network transport. The Flexible Site and InterZone Links feature provides alternative backhaul solutions for these links. The Flexible Site and InterZone Links feature is implemented by creating IP-IP tunnels across a backhaul network.

The use of Ethernet links for ASTRO® 25 system site and InterZone links affords the following benefits:

- Use of a higher bandwidth network to transport ASTRO® 25 system traffic.
- Reuse of the existing Ethernet backhaul network to transport radio communication system traffic (in contrast to the use of dedicated circuits for this purpose).

NOTICE: Conventional flexible site and InterZone links differ to a large extent form trunking links. For details on the conventional links, see the *Conventional Architectures for L or M Core* manual.

1.2 Flexible Site and InterZone Links Connectivity

The following table lists the available connections supporting Flexible Site and InterZone Links.

Table 1: Flexible Site and InterZone Links Connectivity

Site 1	Site 2
ASTRO® 25 system Zone Core	ASTRO® 25 system repeater site
	ASTRO® 25 system IP simulcast prime site
	ASTRO® 25 trunking subsystem prime site
	ASTRO® 25 system high performance data (HPD) site
	ASTRO® 25 system CCGW site (conventional only)
	NM and/or remote console site
	Customer enterprise network
	Another ASTRO® 25 system Zone Core (InterZone)
ASTRO® 25 system IP simulcast prime site	ASTRO® 25 system IP simulcast sub-site
ASTRO® 25 system IP simulcast Primary prime site	ASTRO® 25 system IP simulcast secondary prime site
ASTRO® 25 trunking subsystem prime site	ASTRO® 25 repeater site
	ASTRO® 25 system CCGW site (conventional only)

Table continued…

Site 1	Site 2
	ASTRO® 25 system IP simulcast sub-site
	NM and/or remote console site
	ASTRO® 25 system high performance data (HPD) site

NOTICE: Motorola Solutions supports the use of the IPv6 protocol at any interface made to a Customer Enterprise Network (CEN) and the ones listed in this section. Data subsystem interfaces (IV&D and HPD service interfaces) employ IPv4.
For information on conventional links, see the *L and M Core Conventional Architectures Engineer Guide*.

1.3 Hybrid Site Links Overview

The Hybrid Site Links feature is a flexible way of connecting a redundant zone core to redundant remote sites in ASTRO® 25 systems. The feature allows the creation of redundant connections between the zone core and remote site by using different connection types.

The feature is available in the M2 system configuration, M3 system configuration with Dynamic System Resilience (DSR), and M3 system configuration without DSR. You can use the Hybrid T1/E1 and Ethernet Links feature to connect redundant zone cores to the following site types:

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

The Trunking Subsystem (Tsub) prime site does not support the Hybrid Site Links feature.

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/E1 bandwidth, the Hybrid Site Links feature supports up to two T1/E1 links that are 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.

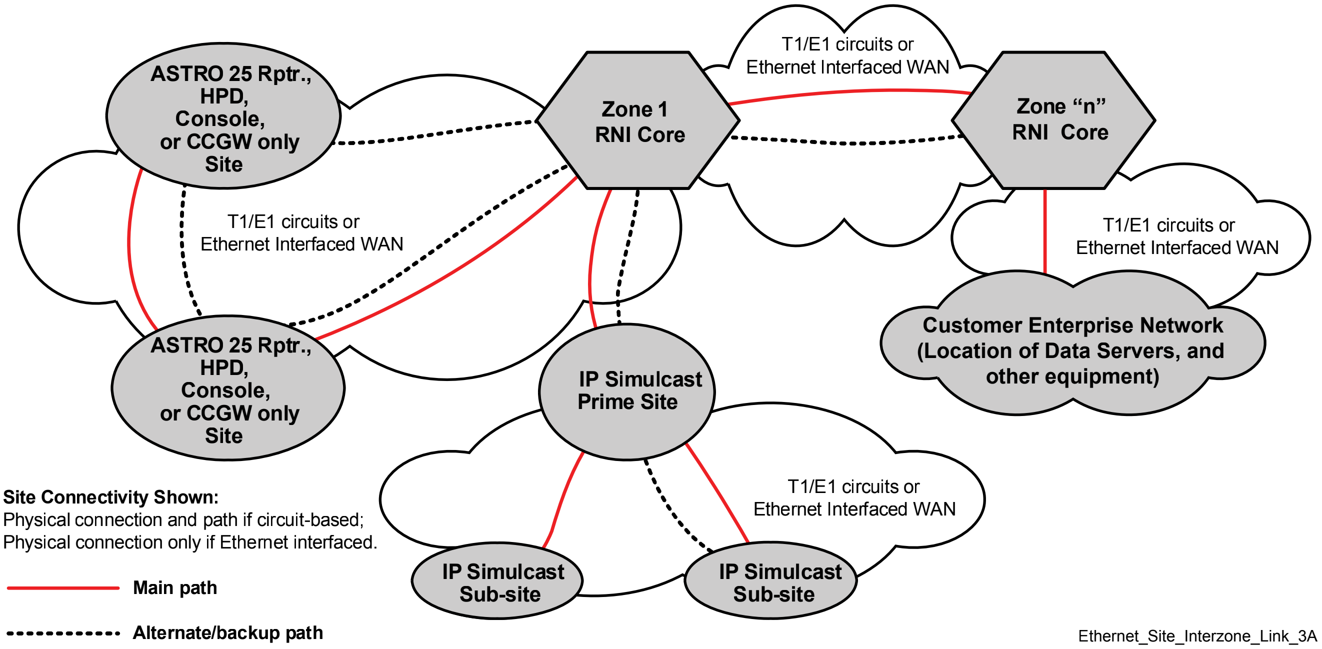
For more information about S6000 core routers and GGM 8000 site gateway transport devices, see the *S6000 and S2500 System Routers* and *GGM 8000 System Gateway* manuals.

1.4 Flexible Site/InterZone Link System

The following figures show links over which Flexible Ethernet connectivity is supported on an ASTRO® 25 system without Dynamic System Resilience. For the DSR version of the figure, see the *Dynamic System Resilience Feature Guide* manual.

NOTICE: The following diagrams assume a non-Tsub configuration. Tsubs only support Ethernet site links between the core site and prime site, and between the prime site and sub-sites.

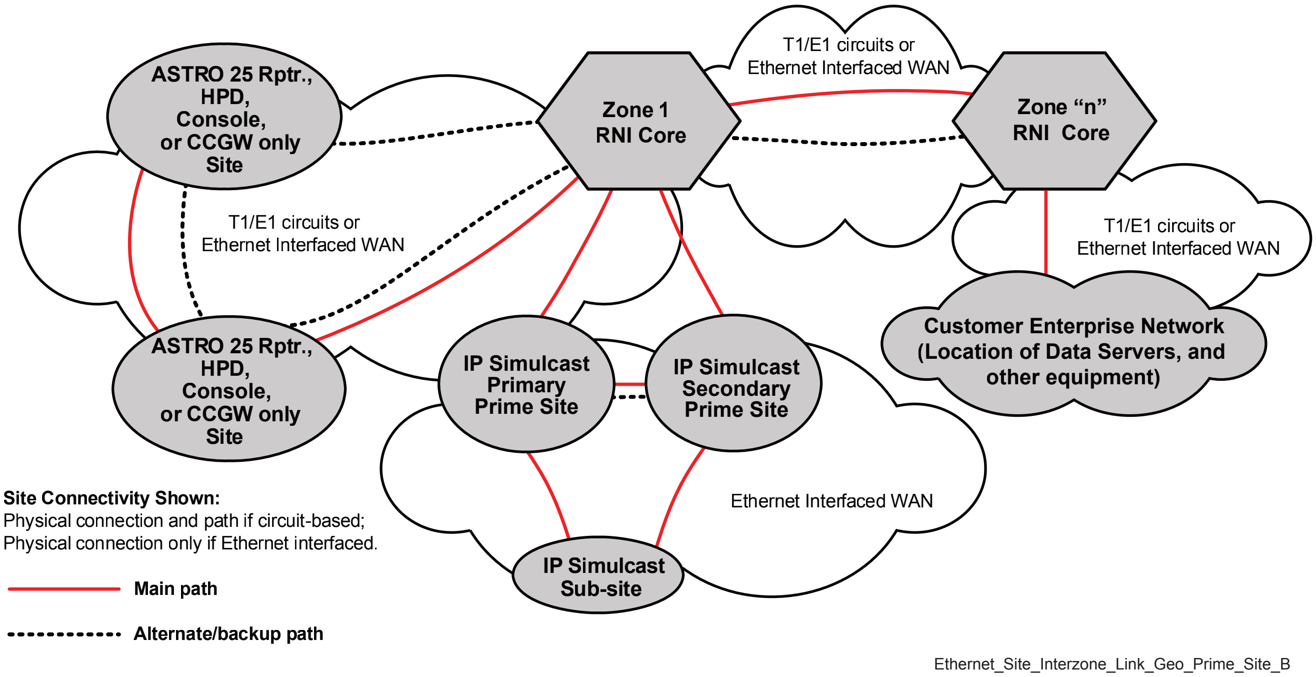
Figure 1: Flexible Site/InterZone Links


ASTRO 25 Rptr., HPD, Console, or CCGW only Site
Zone 1 RNI Core
T1/E1 circuits or Ethernet Interfaced WAN
Zone "n" RNI Core
T1/E1 circuits or Ethernet Interfaced WAN
T1/E1 circuits or Ethernet Interfaced WAN
Customer Enterprise Network (Location of Data Servers, and other equipment)
ASTRO 25 Rptr., HPD, Console, or CCGW only Site
IP Simulcast Prime Site
T1/E1 circuits or Ethernet Interfaced WAN
IP Simulcast Sub-site
IP Simulcast Sub-site
Main path
Alternate/backup path

Site Connectivity Shown:
Physical connection and path if circuit-based;
Physical connection only if Ethernet interfaced.

Ethernet_Site_Interzone_Link_3A

Figure 2: Flexible Site/ InterZone Links – Geographically Separate IP Simulcast Prime Sites


ASTRO 25 Rptr., HPD, Console, or CCGW only Site
Zone 1 RNI Core
T1/E1 circuits or Ethernet Interfaced WAN
Zone "n" RNI Core
T1/E1 circuits or Ethernet Interfaced WAN
T1/E1 circuits or Ethernet Interfaced WAN
Customer Enterprise Network (Location of Data Servers, and other equipment)
ASTRO 25 Rptr., HPD, Console, or CCGW only Site
IP Simulcast Primary Prime Site
IP Simulcast Secondary Prime Site
Ethernet Interfaced WAN
IP Simulcast Sub-site
Main path
Alternate/backup path

Site Connectivity Shown:
Physical connection and path if circuit-based;
Physical connection only if Ethernet interfaced.

Ethernet_Site_Interzone_Link_Geo_Prime_Site_B

1.5 Intra-Prime Site Link

To support the geographic redundancy feature, the Primary Prime Site, and Secondary Prime Site interface through an Intra-Prime Site Extended Ethernet LAN Link. It is supported by two Ethernet LAN Switches that operate over a Layer 2 network with full end-to-end link redundancy.

NOTICE: For a geographically redundant prime site, consider determining the overall “jitter budget” to account for the Intra-Prime Site (Ethernet) link between the Primary Prime Site and Secondary Prime Site. Latency, packet loss, failover performance, and other factors must be considered to ensure proper operation. For details regarding the transport constraints associated with the Intra-Prime Site link, see the *Trunked IP Simulcast Subsystem Prime Site* and *Edge Availability with Wireline Console Feature Guide for Trunking Subsystems* manuals.

1.6 Trunking Subsystem (Tsub) Site Links

This section includes information regarding the type of links supported between the zone core and the Trunking Subsystem (Tsub), and between the Tsub prime site and the subsites.

This configuration provides a single or geographically redundant prime site option and requires Ethernet link support between the WAN backhaul switch at the zone core and the prime site router or gateway. Ethernet link support is between the WAN backhaul switch at a subsite and the remote site access router or gateway at the prime site. T1/E1 site links are not supported.

The Tsub allows for a single site link and dual site links between prime sites and zone cores.

Wide Area Network (WAN) links between the zone core and the Tsub prime site, and WAN links between the Tsub prime site and the Tsub subsites can carry only 10 Mbps of payload traffic. The number of voice streams that can be carried on a 10 Mbps WAN link is dependent on the link type. For example, unencrypted IPv4 links can carry more voice traffic than encrypted IPv4 links.

Additional links in a Tsub are:

- Intra-prime site link (geographically redundant configurations)

1.7 Ethernet Link Characteristics

In cases where an Ethernet link is shared, the resulting (inherent) performance impairments may directly affect ASTRO® 25 system behavior.

Links are characterized during the system or feature planning phase to ensure the required level of performance with Ethernet links. This section discusses important Ethernet link characteristics analyzed when planning the implementation of Flexible Site and InterZone Links.

1.7.1 Latency

Latency does not affect speech quality up to a point. However, it has a direct impact on system access time which manifests itself as truncation and audio throughput delay.

Latency must be understood and quantified for each Ethernet link on the system to meet the system access time requirements. In addition, consider the difference between the source and destination links because asymmetry may be an additional source of truncation.

1.7.2 Inter-Packet Delay Variation (Jitter)

Inter-packet delay variation, also known as jitter, refers to the variation in latency.

Audio performance relies on a constant, steady delivery of voice packets from the source to all the destinations. The ASTRO® 25 system can tolerate certain amounts of jitter by using packet hold-off timers referred to as jitter buffers.

Specifications are established for the amount of jitter that an ASTRO® 25 system can tolerate to ensure a low probability of exceeding the jitter buffers.

1.7.3
Packet Loss

Packet loss may result from exceeding jitter budgets or actual packet loss in the network. IP-based networks are susceptible to packet loss or transient congestion, primarily due to routing component loading or route convergence on failures.

Unlike jitter, packet loss cannot be mitigated and has an immediate impact on speech quality. The probability of packet loss must be kept low to prevent site backhaul-sourced audio quality issues.

1.7.4
Ethernet Site Link Statistics – Transport Devices

For transport devices supporting Ethernet site links (Site Gateway, other) the IPDV (IP Delay Variation) service (service internal to the device as configured) can perform link delay and jitter calculations.

Statistics from these calculations can be used to work with the service provides of the backhaul network to ensure best possible performance.

Performance statistics are obtained at the command line (local access) by executing the following command:

`SHow !<port>-IPDV STATIStics`.

See the *System Gateways – GGM 8000* manual to obtain the command-line prompt for the Site Gateway.

The `SHow -IPDV STATIStics` command calculates and displays delay (IPTD), jitter (IPDV), as well as packet loss (IPLR) statistics and status for the link, like the following:

```
[1]Router_02 # sh -ipdv stat
================= IPDV Statistics V2=========================
State Up
Cause Up
IP address <IP address>
Source IP address <IP address>
Dest IP address <IP address>
            Num Sum          Avg       SumSqMaxMin
IPTD     15         22        1         0 2 0
IPDV     600       600005100       0 - -
IPDV 99
Percentile3        600       200       -   200   0
------ IPLR measurements ------
Number of packets sent from source endpoint      603
Number of packets not received at destination                  0
IP Packet loss rate                      0
```

NOTICE: IPTD and IPDV statistics are reported in milliseconds.

For more information on the Ethernet site links for transport devices, see the *Enterprise OS Software Reference Guide* and the *Enterprise OS Software User Guide*.

NOTICE: The Enterprise OS software is the Operating System (OS) software installed on the Motorola Solutions transport device supporting Ethernet site links.

1.7.5 Ethernet Site Link Statistics – Configuration/Service Software for Comparators

When a GCM 8000 Comparator is employed in the system, link delay measurements can be obtained using the CSS Get Link Delay Feature. This procedure, however, should be repeated several times to verify the accuracy of the link delay measurements from a collection of measurements. The link delay in the conventional comparator for each sub-site can be manually entered into the conventional comparator subsite Configuration tab in the CSS. For more details, see the *CSS Online Help for Comparator* (Local Status Screen).

When an MLC 8000 Comparator is employed in the system, link delay measurements can be obtained with the MLC 8000 Configuration Tool. See the *MLC 8000 Configuration Tool User Guide* manual or online help.

For other information regarding Ethernet site links for comparators, see the *CSS Online Help for Comparator*.

1.8 Ethernet Link Quality – System Impact

Congestion and link impairments (such as latency, jitter, and packet loss) on an Ethernet link may have the following system performance impacts:

- System access time – Various aspects of system access time are as follows:
  - Voice access time – The amount of time that the radio user must wait for the talk permit tone or a grant indication before speaking.
  - Speech truncation – If a user begins speaking before the grant indication (talk permit tone on the subscriber unit), the initial part of the communication is not captured for transmission to the user at the receiving end.
  - Audio throughput delay – Includes the time it takes to transport the audio from the source subscriber or console to all the destinations, and then begin playing it out at the speaker.

  NOTICE: For interzone conventional calls, the access time of voice calls increases due to the additional network delays between zones.
- Data service performance – Reduction in data throughput.

Long system access times can result in a degraded user experience in a half-duplex conversation. The following symptoms could potentially be observed:

- Audio truncation
- Impaired audio quality
- Increased incidence of subscriber retries
- Congestion on the Control Channel

1.9 Network Backbone Requirements

Contact your Motorola Solutions representative for details regarding network backbone requirements.

Chapter 2

Theory of Operations

This chapter provides conceptual information about the Flexible Site and InterZone Links feature and its implementation.

2.1 Ethernet Link Constraints for ASTRO Systems

The following guidelines must be followed when Ethernet links are implemented between zones on an ASTRO® 25 system:

- All InterZone links in a system must be of the same interface type (cannot mix T1/E1 and Ethernet).
- All Ethernet InterZone links in a system must use the same packet prioritization scheme.
- Combining core/exit functions for transport devices is not allowed when T1/E1 InterZone links are needed.

The following guidelines must be followed when Ethernet links are implemented between sites on an ASTRO® 25 system:

- Site links within a zone may be of mixed interface types (Ethernet or T1/E1).
- Both ends of site links must be of the same type (cannot use Ethernet on the Zone Core side and T1/E1 on the remote site side; setting them up conversely is not possible either).
- All Ethernet site links terminated on a core router pair must use the same packet prioritization scheme.
- All subsite links within an IP simulcast subsystem must be of the same type at the Core and Remote Site.
- If dual-site routers are utilized, the backhaul network must provide two network demarcations at the Core and Remote Site.
- Control Room sites cannot support Ethernet backhaul using an S2500 router. Therefore they must be upgraded to an S6000 router or the GGM 8000 gateway that utilize three Ethernet interfaces to support Ethernet Site Links.
- Combining core/exit functions for transport devices is not allowed when T1/E1 InterZone links are needed.
- Motorola Solutions supports the use of the IPv4 at any interface made to a Customer Enterprise Network (CEN), the use of IPv6 for connection endpoints, as well as the site links listed in Flexible Site and InterZone Links Connectivity on page 25. Data subsystem interfaces (IV&D and HPD service interfaces) employ IPv4.
- In Layer 2 networks, each pair of core routers and their associated sites must be a part of the same IP subnet and use the same VLAN ID. The same principle applies to IP simulcast access routers and their associated Subsites and exit router pairs. These restrictions are in place to minimize network congestion and maximize performance.
- In Layer 2 networks, it is possible to implement either HP or Extreme backhaul switches. The private radio system manages both switch types. The configuration of the Extreme switches is handled by Cambium Networks.
- It is recommended that systems with a significant number of sites and/or zones utilize a Layer 3 backhaul design to maximize flexibility.

2.2
Ethernet Link Implementation

The Flexible Site and InterZone Links feature is implemented by creating IP-to-IP tunnels across a backhaul network provided by your organization to transport ASTRO® 25 system radio network infrastructure traffic. Since the ASTRO® 25 system network traffic is encapsulated in a tunnel, your organization does not provide dynamic routing protocol interactions with the backhaul network.

NOTICE: Links supporting IPv6 require encryption on the routers or gateways so that radio network infrastructure traffic is encrypted using IPSec. IPSec encryption is applied to the IPv6 header.

2.2.1
Flexible Ethernet Link Components

The components required to implement the Ethernet links on an ASTRO® 25 system are Zone Core and Prime Site switches, as well as router sets.

NOTICE: In your organization, the router interface is the backhaul demarcation point at remote sites. Remote sites that have dual routers require two backhaul demarcations.

2.2.1.1
Zone Core Switches

The core backhaul LAN switch (HP ProCurve 2620, or, for Layer 2 networks only, Extreme Networks E4G 200 or 400) provides link aggregation and a service tap point in the network.

Up to two switches are required at each Zone Core.

2.2.1.2
Prime Site Switches

The prime site backhaul LAN switch (HP ProCurve 2620, or, for Layer 2 networks only, Extreme Networks E4G 200 or 400) provides link aggregation and a service tap point in the network.

Two switches are required per IP simulcast prime site that utilizes Ethernet subsite links.

For more information, see Backhaul Network Implementation on page 33.

2.2.1.3
Router Sets

Possible router/gateway sets include:

- core – site
- exit – exit
- simulcast access – simulcast subsite

The master site for an M3 core configuration can implement Ethernet links by employing a combined (dual-function) Core/Exit Router supporting IntraZone (zone-to-site) network traffic (Core router) and InterZone (zone-to-zone) network traffic (Exit router), or standalone Core and Exit routers.

All routing functions may be implemented on either an S6000 or a GGM 8000. S6000 and GGM8000 devices may be mixed within a zone core, but both router/gateways in a redundant pair must be of the same model and be configured to perform the same functions.

2.2.2 Physical Interface for Ethernet Connection

The required physical connection for the backhaul network Ethernet interfaces is 10/100Base-T, RJ-45.

NOTICE: For the S2500 router used as a site router, the connection is 10Base-T.

2.2.3 Backhaul Network Requirements

The network requirements for Flexible Site and InterZone Links are defined based on Quality of Service (QoS) mechanisms available on the network. QoS refers to the ability to provide differentiated priorities to applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

QoS guarantees are important in shared networks where capacity is a limited resource. The backhaul network used for Flexible Site and InterZone Links must implement at least two QoS levels. Four QoS levels are recommended for optimal radio user experience.

NOTICE: QoS is required unless the ASTRO® 25 system RNI traffic for a single site link (point to point Ethernet dedicated for ASTRO® 25 system RNI use) is the only traffic on the link.
The Motorola Solutions routers and gateways support QoS mechanisms by default. However, for the Flexible Site and InterZone Links to function properly, additionally configure QoS in your backhaul network.

The Flexible Site and InterZone Links feature supports Layer 2 or Layer 3 Ethernet networks.

NOTICE: The Flexible Site and InterZone Links feature supports Layer 2 and Layer 3 IPv4 backhaul networks provided by your organization. Only Layer 3 backhaul networks provided by your organization are supported for IPv6.

2.2.4 Backhaul Network Implementation

There are several ASTRO® 25 system link configurations for Ethernet links, as described in this section.

NOTICE: All flexible site and InterZone links in a system must utilize the same IP Version. For example, a mixture of IPv4 flexible site and InterZone links and IPv6 flexible site and InterZone links within the same system is **not** a supported configuration.

2.2.4.1 Layer 2 Backhaul Network

In the context of the Flexible Site and InterZone Links feature, Layer 2 networks are networks that implement QoS mechanisms at Layer 2 through IEEE 802.1Q user priority (such as Carrier Ethernet). Layer 2 backhaul implementations are illustrated in:

- Zone Core – Core Router to Site Router – Layer 2 Backhaul Implementation on page 35
- Prime Site Access Router to Subsite Router – Layer 2 Backhaul Implementation on page 36

NOTICE: It is recommended that two connections are provided from your organization's backhaul network to the core backhaul switches, as shown in:

- Zone Core – Core Router to Site Router – Layer 2 Backhaul Implementation on page 35
- Prime Site Access Router to Subsite Router – Layer 2 Backhaul Implementation on page 36

However, it is possible to implement a single interface to the backhaul network. When a single gateway is provided by the backbone supplied by your organization, both core backhaul switches are still used and are configured with a single interface to your organization's gateway connection. Also, an additional VLAN must be trunked between the backhaul switches to provide core/exit router path redundancy to your organization's network. The core backhaul switches in the following sections do not have Spanning Tree Protocol enabled. It is recommended for the demarcation point for your organization's backhaul to implement the Spanning tree Protocol to mitigate Layer 2 loops. Backhaul design is the responsibility of your organization and your organization's service providers. See:

- Zone Core – Core Router to Site Router – Layer 2 Backhaul Implementation on page 35
- Prime Site Access Router to Subsite Router – Layer 2 Backhaul Implementation on page 36

2.2.4.2 Layer 3 Backhaul Network

In the context of the Flexible Site and InterZone Links feature, Layer 3 networks are networks that implement QoS mechanisms at Layer 3 through the IP Precedence field (RFC 791) or the IP Differentiated Services field (RFC 2474, 2780, and 3260). For illustrations of Layer 3 backhaul implementations, see:

- Zone Core – Core Router to Site Router – Layer 3 Backhaul Implementation on page 37
- Prime Site Access Router to Subsite Router – Layer 3 Backhaul Implementation on page 38

NOTICE: It is required for two connections to be obtained from your organization's backhaul network to the core backhaul switches, as shown in:

- Zone Core – Core Router to Site Router – Layer 3 Backhaul Implementation on page 37
- Prime Site Access Router to Subsite Router – Layer 3 Backhaul Implementation on page 38

However, it is possible to implement a single interface to the backhaul network. When a single interface is implemented, both core backhaul switches are still used with a connection to switch 1. Also, an additional VLAN must be configured between the backhaul switches. The core backhaul switches listed in the following sections do not have Spanning Tree Protocol enabled:

- Zone Core – Core Router to Site Router – Layer 3 Backhaul Implementation on page 37
- Prime Site Access Router to Subsite Router – Layer 3 Backhaul Implementation on page 38

The demarcation point for your organization's backhaul must not implement additional switches that could cause Layer 2 loops.

2.2.4.3 Mixed Layer 2 – Layer 3 Backhaul Network

Zone Core – Core Router to Site Router – Mixed Layer 2 and Layer 3 Implementation on page 39 illustrates a mixed Layer2 and Layer3 implementation. This type of implementation requires unique pairs of core routers for Layer 2 sites and Layer 3 sites, since Layer 2 and Layer 3 sites cannot be supported on the same pair of core routers.

NOTICE: The core backhaul switches in Zone Core – Core Router to Site Router – Mixed Layer 2 and Layer 3 Implementation on page 39 do not have Spanning Tree Protocol enabled. The demarcation point for your organization's backhaul must not implement additional switches that could cause Layer 2 loops.

2.2.4.4 Example Network Diagrams

The example network diagrams show both Single Link and Dual Link configurations.

Routers listed in the following sections, numbered as Router 1, Router 2, and Router 3, are examples of "Single Link" connections to repeater sites and or IP simulcast prime sites:

- Zone Core – Core Router to Site Router – Layer 2 Backhaul Implementation on page 35
- Zone Core – Core Router to Site Router – Layer 3 Backhaul Implementation on page 37

The two routers numbered as Router 4 are examples of "Dual Link" connections to a single repeater site or a single IP simulcast prime site.

The routers numbered as Router 1, Router 2, and Router 3 in following sections are examples of "Single Link" connections to IP simulcast subsites:

- Prime Site Access Router to Subsite Router – Layer 2 Backhaul Implementation on page 36
- Prime Site Access Router to Subsite Router – Layer 3 Backhaul Implementation on page 38

The two routers numbered as Router 4 are examples of "Dual Link" connections to a single IP simulcast subsite.

The core routers at the top of the diagrams in following sections are Zone Core core router 1 and 2:

- Zone Core – Core Router to Site Router – Layer 2 Backhaul Implementation on page 35
- Zone Core – Core Router to Site Router – Layer 3 Backhaul Implementation on page 37

The access routers at the top of the diagrams in following sections are prime site access router 1 and 2:

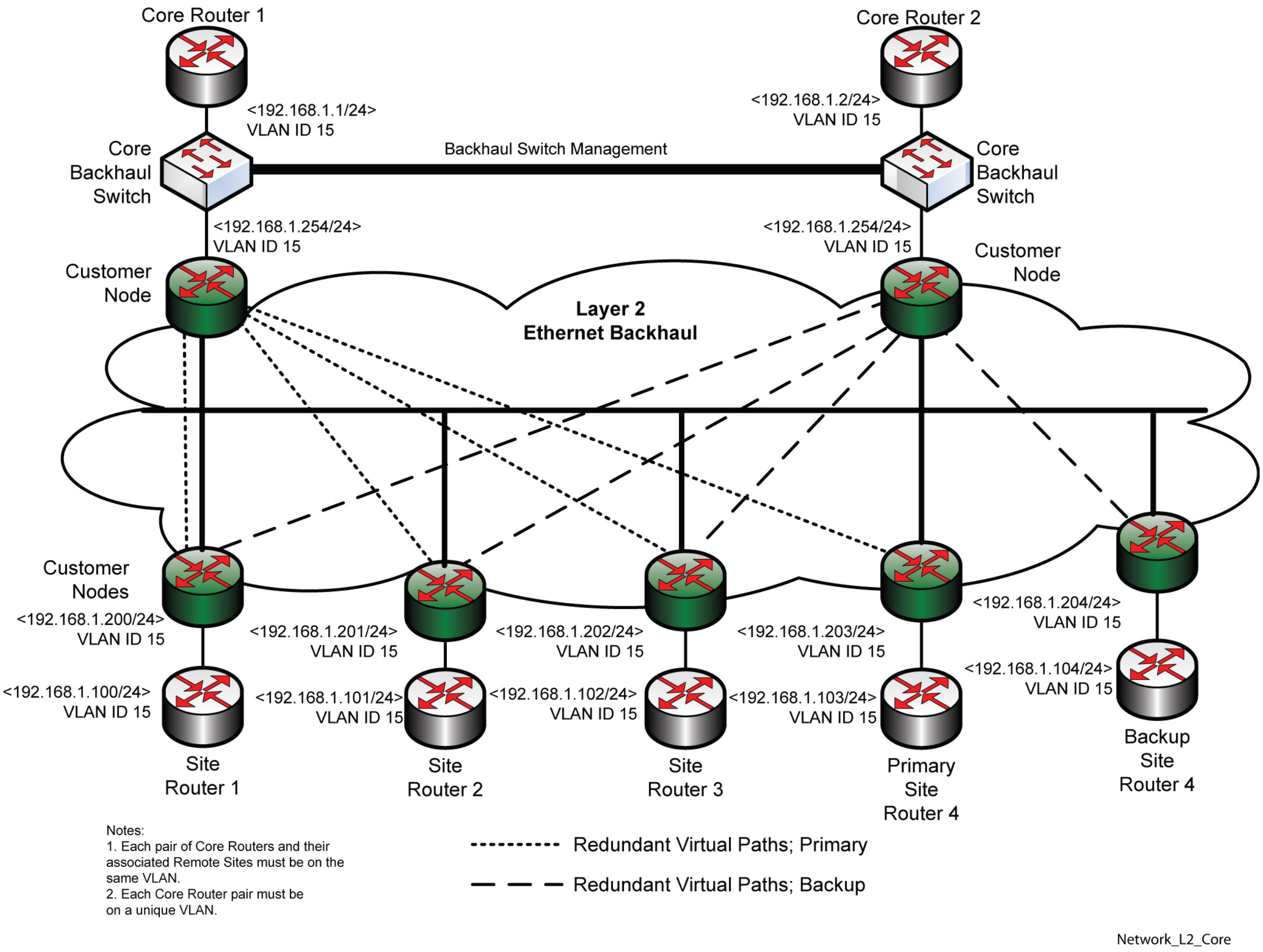
- Prime Site Access Router to Subsite Router – Layer 2 Backhaul Implementation on page 36
- Prime Site Access Router to Subsite Router – Layer 3 Backhaul Implementation on page 38

For Zone Core – Core Router to Site Router – Mixed Layer 2 and Layer 3 Implementation on page 39, the core routers at the top of the diagram are Zone Core core router 1, 2, 3, and 4.

2.2.4.5 Zone Core – Core Router to Site Router – Layer 2 Backhaul Implementation

IMPORTANT: This diagram is an **example**. The IP addresses are shown for illustrative purposes only. Do not use them for system configuration. The numbering is generic and not part of the actual IP addresses used in a system.
Also, the term Router is used in these diagrams to indicate a type of transport functionality, not a specific model of device which can vary depending on system configuration.

Figure 3: Zone Core – Core Router to Site Router – Layer 2 Backhaul Implementation



Notes:
1. Each pair of Core Routers and their associated Remote Sites must be on the same VLAN.
2. Each Core Router pair must be on a unique VLAN.

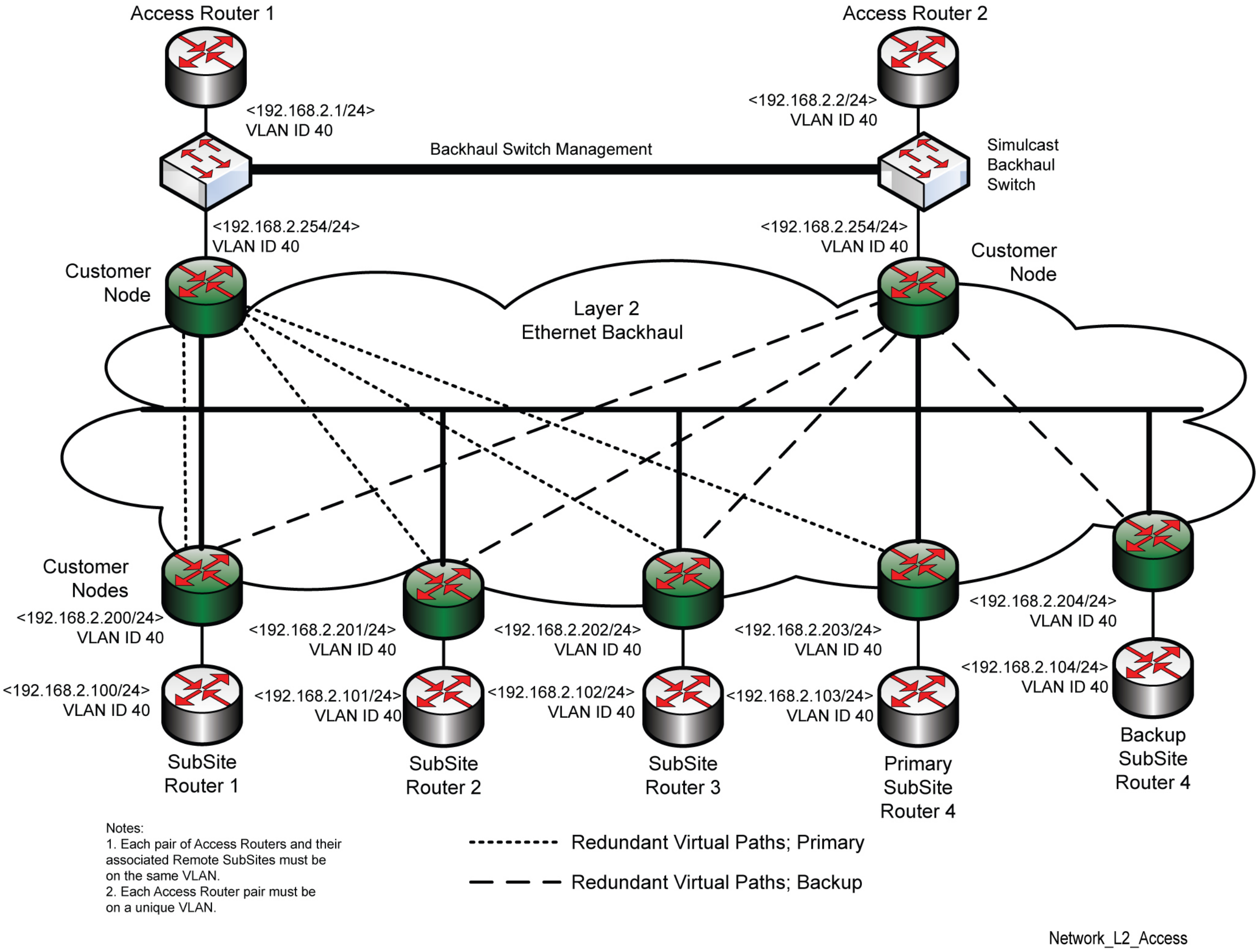
2.2.4.6

Prime Site Access Router to Subsite Router – Layer 2 Backhaul Implementation

IMPORTANT: This diagram is an **example**. The IP addresses are shown for illustrative purposes only. Do not use them for system configuration. The numbering is generic and not part of the actual IP addresses used in a system.

Also, the term Router is used in these diagrams to indicate a type of transport functionality, not a specific model of device which can vary depending on system configuration.

Figure 4: Prime Site Access Router to Subsite Router – Layer 2 Backhaul Implementation



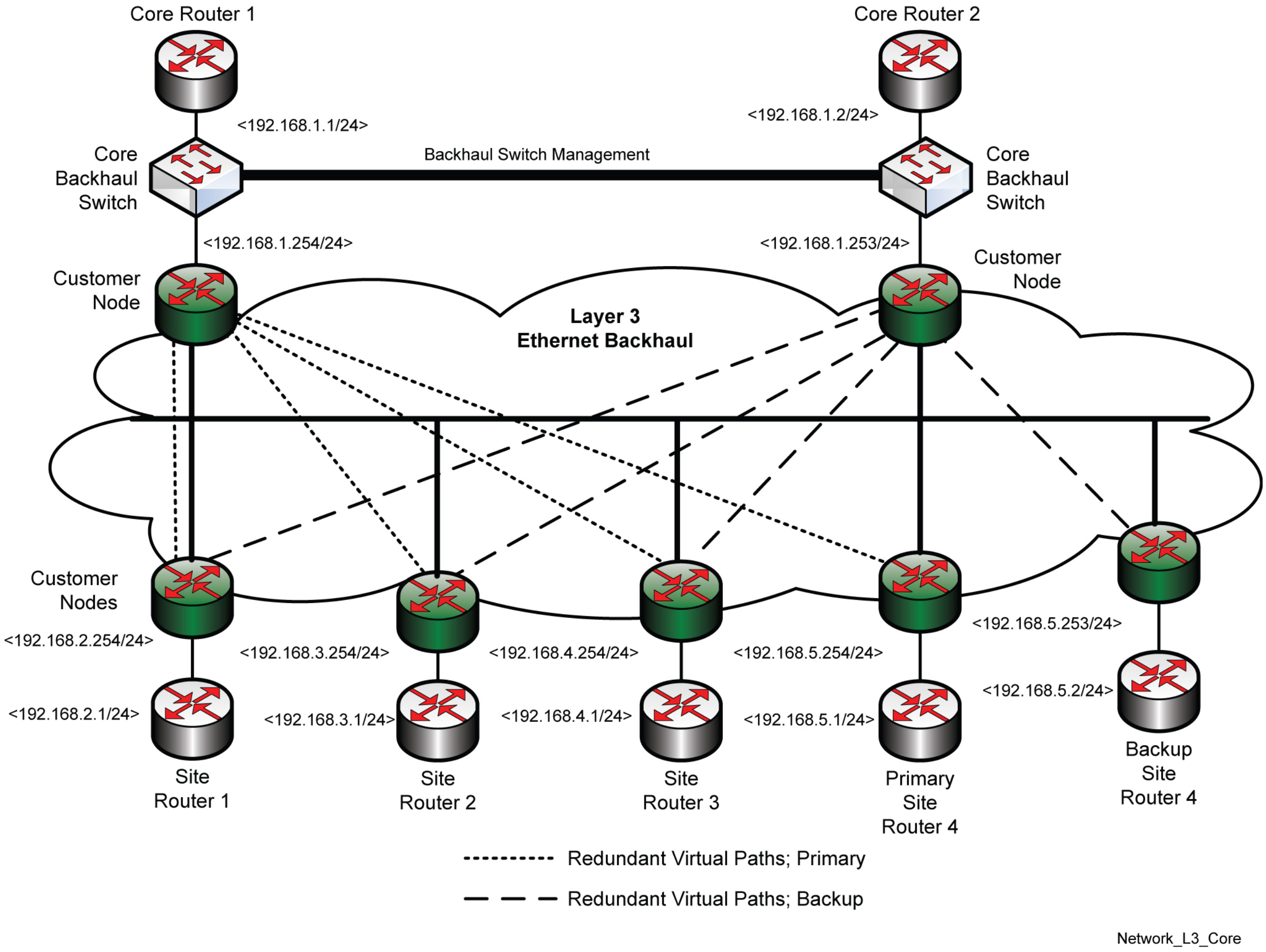
2.2.4.7

Zone Core – Core Router to Site Router – Layer 3 Backhaul Implementation

IMPORTANT: This diagram is an **example**. The IP addresses are shown for illustrative purposes only. Do not use them for system configuration. The numbering is generic and not part of the actual IP addresses used in a system.

Also, the term Router is used in these diagrams to indicate a type of transport functionality, not a specific model of device which can vary depending on system configuration.

Figure 5: Zone Core – Core Router to Site Router – Layer 3 Backhaul Implementation



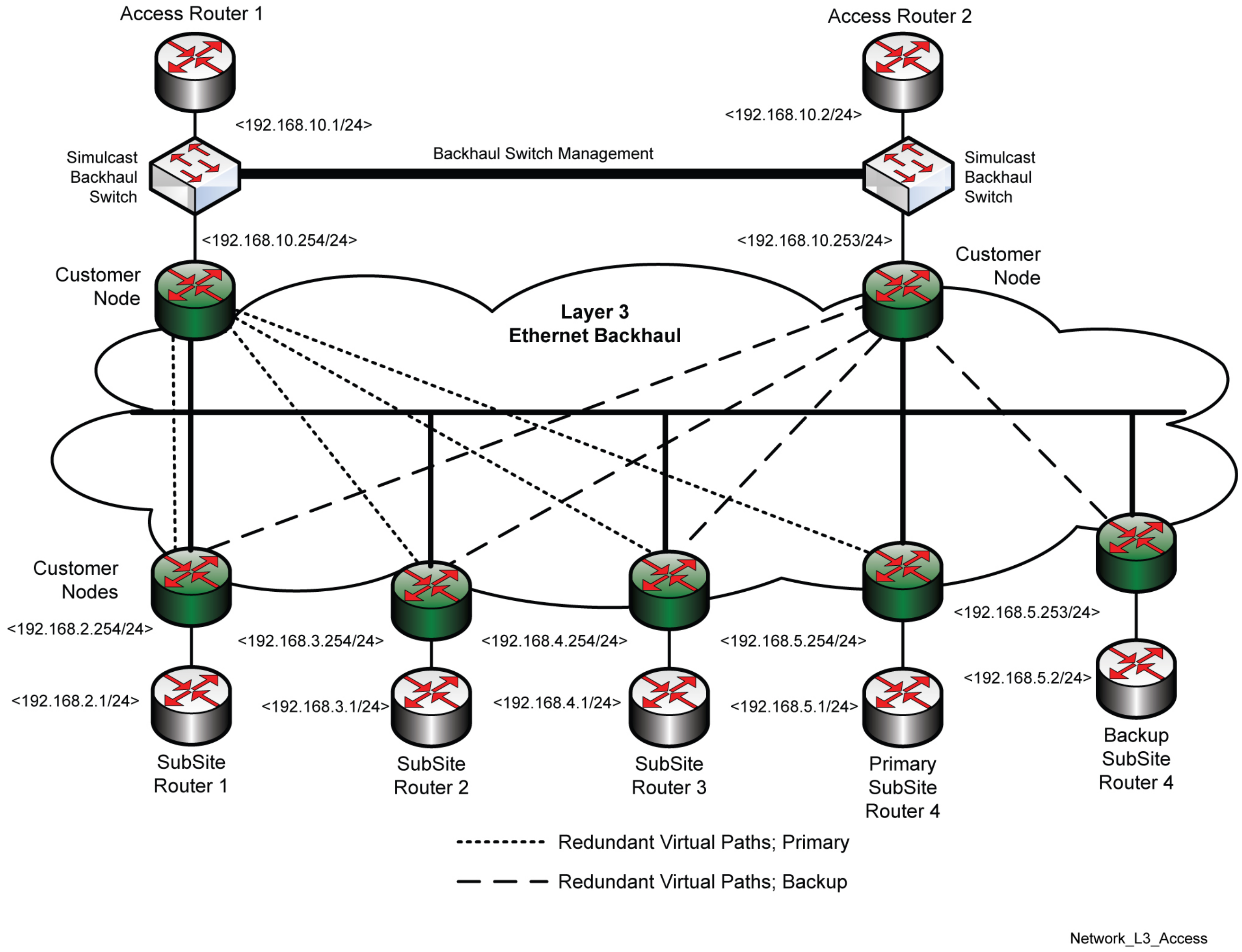
2.2.4.8

Prime Site Access Router to Subsite Router – Layer 3 Backhaul Implementation

IMPORTANT: This diagram is an **example**. The IP addresses are shown for illustrative purposes only. Do not use them for system configuration. The numbering is generic and not part of the actual IP addresses used in a system.

Also, the term Router is used in these diagrams to indicate a type of transport functionality, not a specific model of device which can vary depending on system configuration.

Figure 6: Prime Site Access Router to Subsite Router – Layer 3 Backhaul Implementation

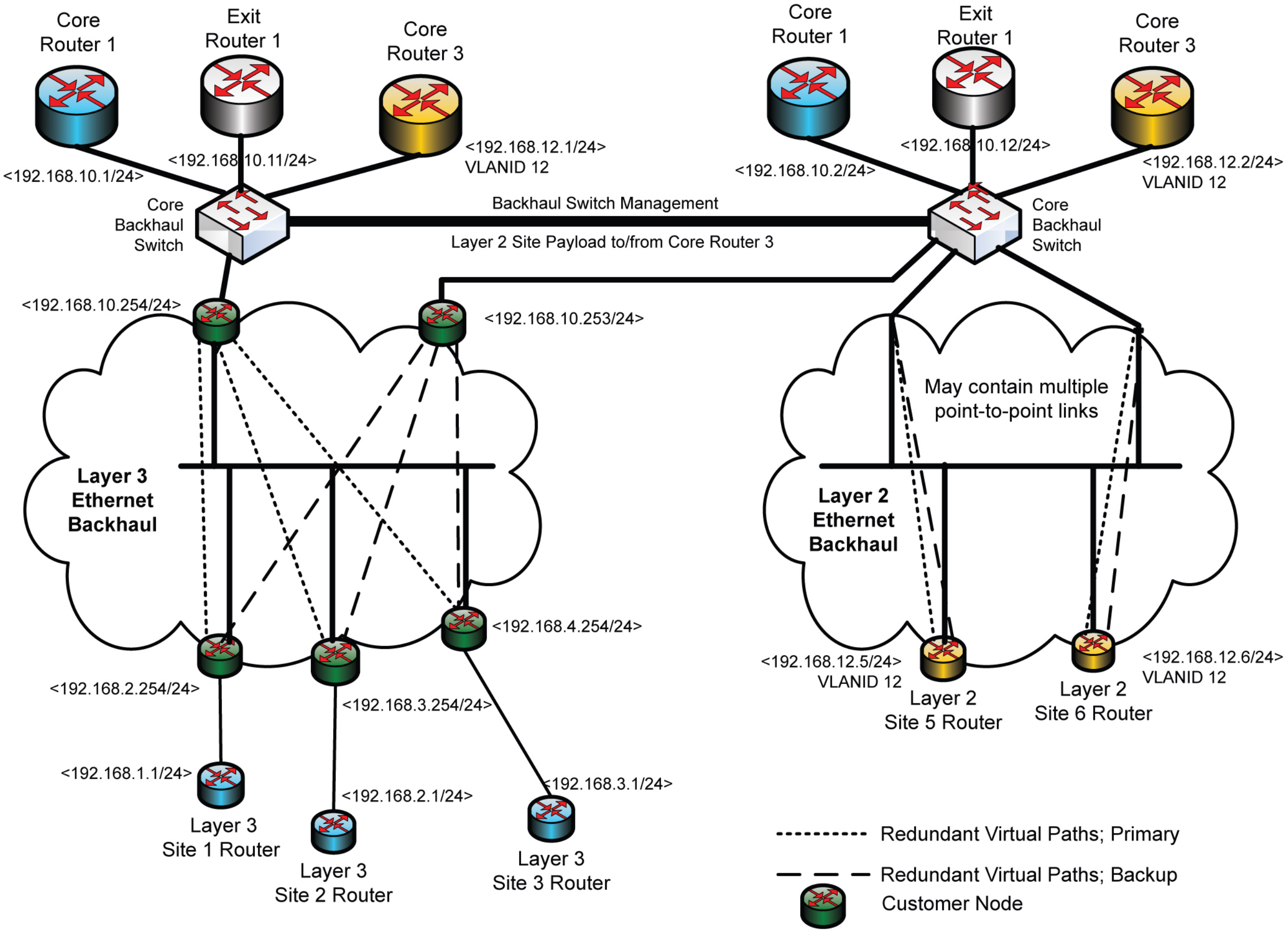


2.2.4.9 Zone Core – Core Router to Site Router – Mixed Layer 2 and Layer 3 Implementation

IMPORTANT: This diagram is an **example**. The IP addresses are shown for illustrative purposes only. Do not use them for system configuration. The numbering is generic and not part of the actual IP addresses used in a system.

Also, the term Router is used in these diagrams to indicate a type of transport functionality, not a specific model of device which can vary depending on system configuration.

Figure 7: Zone Core – Core Router to Site Router – Mixed Layer 2 and Layer 3 Implementation



Network_L2_L3_combo

NOTICE: There are limitations to layer 2 and 3 and mixed implementations, depending on whether the transmitted network traffic is based on IPv4 or IPv6. For details, contact your Motorola Solutions field engineer.

2.3 IP Traffic Prioritization Across Ethernet Links

The ASTRO® 25 system routinely prioritizes packets, as they traverse through the system, as defined for various system components and applications. If Ethernet links are used, packet priorities within the ASTRO® 25 system must be mapped to the appropriate QoS levels provided by the user's network using the Layer 2 mechanisms (for example, 802.1p) or Layer 3 mechanisms (for example, IP precedence bits). Your organization provides the mapping information during the system planning phase.

NOTICE: Under normal conditions, the system functions properly with two, three, or four QoS levels. However, it is recommended for the backhaul network to provide four QoS levels. Less than four could result in degraded user experience for some system applications, due to other traffic, insufficient bandwidth, or congestion on the network.
For IPv6 Flexible Site and InterZone Links, traffic priority is indicated by the Traffic Class Field in the IPv6 header rather than the Type of the Service field in the outermost IPv4 header.

2.4 IP Addressing for Ethernet Links

The tunnel endpoints for each Ethernet link require IP addresses routable on the backhaul network. The endpoints are configured with IP addresses that match the IP addressing scheme of the backhaul network either for IPv4 or IPv6 address schemes.

When configuring IPv6 addresses for the IPv6 Flexible Site and InterZone Links feature, a fixed 64-bit subnet mask is enforced. Attempts to use IPv6 with backhaul networks configured with a subnet masks greater than 64 bits may result in the failure to properly route ASTRO® 25 system RNI application traffic, which would result in a catastrophic site and InterZone link failure.

See the Motorola Solutions custom configuration documentation for IP addresses specific to the installation.

2.5 Link Security

Link security may be implemented at ASTRO® 25 system demarcation points, using the Link Encryption and Zone Core Protection system features.

Table 2: Link Security Features for Ethernet Links

Feature	Description
Link Encryption	Provides encryption of IP-to-IP tunnels created across the backhaul network using IPSec. The Flexible Site and InterZone Links feature does not require any additional work for router configuration other than what is covered in the *Link Encryption and Authentication* manual.
Zone Core Protection	Provides additional components and functionality for the Zone Core. The Flexible Site and InterZone Links feature does not require any additional configuration procedures other than what is covered in the *Zone Core Protection Infrastructure* manual.

This page intentionally left blank.

Chapter 3

Installation and Configuration

This chapter details the installation process for components required to implement the Flexible Site and InterZone Links feature.

3.1 Prerequisites for the Ethernet Link Installation

The implementation of Ethernet links at the Zone Core and various other sites involves hardware installation and cabling, as well as the use of network management applications for configuration tasks. Read through the installation procedures and plan the installation ahead of time to minimize trips to and from various Zone Core, prime site, and remote site locations.

The following are preparatory steps that should be performed in advance to ensure that the installation proceeds smoothly:

- Ensure that the routers, gateways and switches are installed, cabled to the appropriate ASTRO® 25 system site equipment, and configured with an IP address at each site. For specific procedures, see the installation and initial configuration instructions included in the ASTRO® 25 system documentation CD for these devices.
- Load router, gateway, and switch OS images and Ethernet link-specific configuration files for these devices on the UNC. They can then be “pushed” to the devices once they are available on the network. See the *Unified Network Configurator* manual for information on loading OS images and configuration files.
- Port layouts are provided to the installer who implements the router or gateway cabling at the sites. They are included in the Motorola Solutions custom configuration documentation for your system. Contact your system administrator to obtain these layouts.

3.2 Setting Up Ethernet Links at the Zone Core – Prerequisites

Review the following assumptions and considerations to set up Ethernet links at the Zone Core:

- Ethernet network connectivity to the provider’s backhaul network is functional at the Zone Core.
- The S6000 core routers and exit routers, and the GGM 8000 gateways (M series core) or GGM core gateways (L zone core, K zone core) have been assigned the appropriate IP addresses (loaded at the factory). See the *S6000 and S2500 System Routers* manual and the *GGM 8000 System Gateway* manual for details.
- The two core backhaul switches are installed in a rack, configured for the specific backhaul implementation, and are ready to be cabled for Ethernet links.
- The routers or gateways have been discovered in the Unified Network Configurator (VoyenceControl), using the IP address (node) or subnet discovery, and are ready for configuration management by the UNC application. See the *Unified Network Configurator* manual for details.

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

- Router, gateway, and switch configuration files have been loaded on the UNC. Motorola Solutions provides configuration files that are specific to the Ethernet links implementation on your system. See the *Unified Network Configurator* manual for details.

IMPORTANT: The backhaul switches are not fully configured using any tools. Once both your organization and your service provider supply the backhaul switch configuration information, Motorola Solutions representatives complete the configuration for these devices.

- Port layout information is available to the installer. Contact your system administrator for this information.

NOTICE: A pair of S6000 core routers used for Ethernet site links may also support T1/E1 sites through a Cooperative WAN Routing (CWR) configuration.
A terminal server is configured to provide serial access to routers, gateways, switches (including backhaul switches), and other devices. For more information, see the *Terminal Servers LX Series* and *Service Access Architecture* manuals.

3.2.1
Setting Up Ethernet Links at the Zone Core

When and where to use:
This procedure describes how to set up Ethernet links at the Zone Core (new sites only) for the following:

- Links from the Zone Core to other sites within the zone (core routers)
- Links from one Zone Core to another (exit routers)

Procedure:

1. From the NM client, double-click the **Unified Network Configurator** (UNC) application shortcut and log on using the administrator account name and password.
2. In the **Dashboard** window, select the **Network View** tab.
3. To open the list of available routers (M core) or gateways (L core) in the UNC, perform the following operations:
   a. From **Networks** in the navigation pane, select **ASTRO 25 Radio Network**.
   b. From the list of options in the navigation pane, select **Workspaces**.
   c. From the list of options, double-click the folder with the router and gateway configurations.

      The folder expands to display the list of options.

   NOTICE: To change the view, click **Table** on the toolbar.
4. Select the routers or gateways to which you want to load the configuration files from the **Selected Device** list.

   NOTICE: Push down the configuration files now, but do not reboot the routers or gateways. Do not select the option to reload the routers or gateways in the UNC.
5. Right-click the selected routers or gateways.
6. From the pop-up menu, select **Schedule**.
7. In the **Schedule Push Job** dialog box, type a name for the job in the **Job Name** field.
8. Select the **Task** tab.
9. Select **PushtoStart** in the **Push type** field.
10. Click **Approve & Submit**.

    NOTICE: If needed, press F5 to refresh the window.

11 Press F7.

NOTICE: The configuration push to the device takes approximately 1 minute to complete. If the push is successful, the state for the device appears as `Completed` and a green dot appears next to the device. If the push fails, the state of the device appears as `Failed` and a red dot appears next to the device.

The **Schedule Manager** dialog box appears. If the dialog box does not automatically refresh, press F5.

12 For the core and exit routers (M core) or core gateways (L core), connect ports as follows:

- Connect port 3 on the odd-numbered routers or gateways to the appropriate port on the odd-numbered core backhaul switch
- Connect port 3 on the even-numbered routers or gateways to the even-numbered core backhaul switch.

NOTICE: The switch ports to use for the core backhaul switch connections are included in the Motorola Solutions custom configuration documentation for your system. The appropriate router or gateway ports are mapped in the switch configuration files also provided by Motorola Solutions. Contact your system administrator for these port layouts.

13 Reboot each router or gateway.

14 Launch the Unified Event Manager (UEM) from the NM client, and log on using the administrator account name and password.

15 Follow these steps:

a In the UEM main window, select **Tools** → **Discovery Configuration**.

The **Discovery Configuration** window appears, and the **Site/Network Discovery** tab is selected by default.

b Select the appropriate network type from the **Discovery Type** drop-down list, using the information listed in Discovery Type Parameters on page 46.

c In the **Site ID** field, type the site ID. For details, see Discovery Type Parameters on page 46.

d Click **Start Discovery**.

The **Discovery Status** dialog box appears with the job number for the discovery.

e Click the **View Job Stat**.

f In the **Job View** dialog box, track the job to verify that the devices appear in the log.

NOTICE: You can view the log to verify that all the devices were discovered. The log ends with the following message:

```
Job Status Success
```

Postrequisites:

IMPORTANT: After the Ethernet links are established:

- The Link Encryption feature must be enabled on the S6000 and S2500 routers, and GGM 8000 gateways.
- The Port Security feature must be enabled on the switches.

If Link Encryption and/or Port Security are already implemented, the features must be disabled on the relevant devices before performing the procedures in this chapter.

3.2.2

Discovery Type Parameters

Discovery Type Parameters are parameters for each discovery type. If you select a particular discovery type, some parameters are disabled (you cannot select any values for them). Other parameters have a limited range of values.

Table 3: Discovery Type Parameters

DiscoveryType	Zone ID	MultiSite Options	SiteID	Remote Site IDs
RF Site	unavailable	unavailable	1–150	unavailable
IP Multisite Subsystem	unavailable	Prime Site	1-64	unavailable
		Prime and Remote Sites	1-64	1-32
		Remote Site	1-64	1-32
Circuit Multisite Subsystem	unavailable	Prime Site	1-64	unavailable
		Prime and Remote Sites	1-64	1-15
		Remote Site	1-64	1-15
Console Site	unavailable	unavailable	1001-1191 or 1227-1230	unavailable
Primary Zone Core	unavailable	unavailable	unavailable	unavailable
Backup Zone Core	unavailable	unavailable	unavailable	unavailable
Primary Operations Support Systems	unavailable	unavailable	unavailable	unavailable
Backup Operations Support Systems	unavailable	unavailable	unavailable	unavailable
DSR Shared Network Devices	1-7	unavailable	unavailable	unavailable
Conventional Subsystem	unavailable	unavailable	1-47 Parameter name changes to Conventional Subsystem ID	1-255 Parameter name changes to Conventional Location ID
Backhaul Subsystem	unavailable	unavailable	unavailable	unavailable

Table continued…

DiscoveryType	Zone ID	MultiSite Options	SiteID	Remote Site IDs
Customer Enterprise Network	unavailable	unavailable	unavailable	unavailable

NOTICE:
UEM arrives at the list of device IPs or a range of IPs for the selected discovery type, based on the system System Configuration Plan. Provide the required information.

UEM attempts the discovery of all IP addresses, based on the list of device IP addresses derived from the System Configuration Plan. However, some IP addresses (devices) may not exist in the network. Check the Discovery Logs by selecting the Discovery Job in the Job Status View. It allows you to view details on IP addresses that are discovered and IP addresses that are not reachable. Confirm that IP addresses that are not reachable are not configured in the network. Check the network plan or execute an Internet Control Message Protocol (ICMP) ping on the unreachable IP addresses.

3.3 Setting Up Ethernet Links at a Site – Prerequisites

Review the following assumptions and considerations to set up Ethernet links:

- Ethernet network connectivity to the provider’s backhaul network is functional at the site.
- The S2500 routers with an Ethernet module (alternatively, S6000 routers, or GGM 8000 gateways) are racked at the site and have been assigned the appropriate IP addresses. For details, see the *S6000 and S2500 System Routers* and *GGM 8000 System Gateway* manuals.
- The routers or gateways have been discovered in the Unified Network Configurator (VoyenceControl) using the IP address (node) or subnet discovery, and are ready for configuration management by the UNC application. See the *Unified Network Configurator* manual for details.
- Router, gateway, and switch configuration files have been loaded on the UNC. Motorola Solutions provides configuration files that are specific to the implementation of Ethernet links on your system. See the *Unified Network Configurator* manual for details.
- If the site is an IP simulcast prime site, the two prime site backhaul switches are installed in a rack and are ready to be cabled for Ethernet links.
- Port layout information is available to the installer. Contact your system administrator for this information.

NOTICE: One physical connection is made to the Ethernet backhaul for single-linked sites, and two are established for dual-linked sites. The Core always requires two demarcations, while sites can be single or dual, depending on the site architecture.
Before the UNC is used to deploy configurations to establish Flexible Site and InterZone Links, those sites must be Flexible Site and InterZone Links capable.

A terminal server at the Zone Core and an IP simulcast prime site (if present) is configured (configuration file, menu file, port assignments) to provide serial access to routers, gateways, switches (including backhaul switches) and other devices. See the *Terminal Servers LX Series* and *Service Access Architecture* manuals for more information.

3.3.1 Setting Up Ethernet Links at a Site

Perform this procedure to set up Ethernet links at the following sites:

- ASTRO® 25 system repeater site
- ASTRO® 25 system IP simulcast prime site

- ASTRO® 25 system IP simulcast sub-site
- High Performance Data (HPD) site
- ASTRO® 25 system Conventional Channel Gateway (CCGW) site
- Network Management (NM) and/or remote console site
- ASTRO® 25 system Zone Core InterZone link (zone core in a different zone)

Motorola Solutions supports the use of the IPv4 and IPv6 protocols at any interface made to a Customer Enterprise Network (CEN) and those listed. Data subsystem interfaces, Integrated Voice and Data (IV&D), and HPD service interfaces employ IPv4.

Procedure:

1. From the NM client, double-click the **Unified Network Configurator** (UNC) application shortcut and log on using the administrator account name and password.
2. From the **Dashboard** window, select the **Network View** tab.
3. From the UNC window, open the list of available routers and gateways by following these steps:
   a. From **Networks** in the navigation pane, select **ASTRO 25 Radio Network**.
   b. From the expanded list of options in the navigation pane, select **Workspaces**.
   c. From the expanded list of options, double-click the folder with the router and gateway configurations.

      The folder expands to display the list of options.

   To change the view, click **Table** on the toolbar.
4. Select the routers or gateways to which you want to load the configuration files in the **Selected Device** list.

   Push down the configuration files at this time, but do not reboot the device. Do not select the option to reload the devices in the UNC.
5. Right-click the selected routers or gateways.
6. From the pop-up menu, select **Schedule**.
7. In the **Schedule Push Job** dialog box, in the **Job Name** field, type a name for the job.
8. Select the **Task** tab.
9. In the **Push type** field, select **PushtoStart**.
10. Click **Approve & Submit**.

    To refresh the window with any updates, press F5.
11. Press F7. If the dialog box does not automatically refresh, press F5.

    The configuration push to the device completes in approximately 1 minute. If the push is successful, the state for the device appears as `Completed` and a green dot appears next to the device. If the push fails, the state of the device appears as `Failed` and a red dot appears next to the device.

    The **Schedule Manager** dialog box appears.
12. Perform the following operations:

    NOTICE: The switch ports to use for the prime site backhaul switch connections are included in the custom configuration documentation Motorola Solutions provided for your system. The appropriate router or gateway ports are mapped in the switch configuration files Motorola Solutions also provided. Remote site connections vary, based on the implementation. Contact your system administrator for the port layouts.

If…	Then…
If S2500 routers are used at the remote site,	perform the following actions: **a** Replace the T1/E1 module with the Ethernet module. **b** Connect port 2 on each site router (S2500) to the appropriate port on the Ethernet backhaul service provider device. This device may be a switch or a router, depending on your implementation.
If S6000 Routers or GGM 8000 Gateways are used at the remote site,	connect port 3 on each site router or site gateway to the appropriate port on the Ethernet backhaul service provider device. This device may be a switch or a router, depending on your implementation.
If you are in a simulcast prime site,	connect port 3 on each S6000 Router or GGM 8000 Gateway to the appropriate ports on the Ethernet backhaul switches.

13 Reboot the site routers or site gateways.

Reboot the site router or site gateway at the site, as it cannot be done from the UNC.

14 Verify that the site link is operational. Test for wide-area call capability.

15 Launch the Unified Event Manager (UEM) from the NM client, and log on using the administrator account name and password.

16 Perform the following actions:

a In the UEM main window, select **Tools → Discovery Configuration**.

The **Discovery Configuration** window appears, and the **Site/Network Discovery** tab is selected by default.

b Select the appropriate network type from the **Discovery Type** drop-down list.

c In the **Site ID** field, type the site ID.

d Click **Start Discovery**.

The **Discovery Status** dialog box appears with the job number for the discovery.

e Click **View Job Stat**.

The **Job View** dialog box appears and you can track the job.

f View the log to verify that all the devices were discovered. The log ends with the following message: `Job Status Success`.

17 From the NM client, launch the UNC and log on using the administrator account name and password.

18 Perform the following actions to rediscover devices in the UNC:

a In the UNC main window, press F7.

The **Schedule Manager** window appears in the UNC with the discovery jobs displayed.

b Verify that all devices at the selected site appear in the appropriate zone and the appropriate site in the UNC window.

If an HPD site is colocated with the ASTRO® 25 system repeater site, verify that the HPD site controllers and base radios appear in the appropriate zone and site in the UNC window.

Postrequisites:

IMPORTANT: After the Ethernet links are established:

- The Link Encryption feature must be enabled on the S6000 and S2500 Routers, and GGM 8000 Gateways.
- The Port Security feature must be enabled on the switches.

If Link Encryption and/or Port Security are already implemented, the features must be disabled on the relevant devices before performing the procedures in this chapter.

3.3.2

Enabling Link Encryption and Ethernet Port Security

Once the router, gateway, and switch equipment is installed and configured at the master and remote sites, verify the integrity of each link.

NOTICE: Links supporting IPv6 require link encryption so that radio network infrastructure traffic is encrypted using IPSec. IPSec encryption is applied to the IPv6 header.

Chapter 4

Optimization

This chapter covers optimization in relation with the Flexible Site and InterZone Links feature.

4.1 Optimization for Ethernet Site Links

To optimize the performance of the system, keep component firmware up-to-date as a baseline for your system.

There are no optimization procedures applicable to the Flexible Site and InterZone Links feature. Links are implemented after the analysis of network characteristics during the system planning phase.

This page intentionally left blank.

Chapter 5

Operation

This chapter details tasks typically performed after the Flexible Site and InterZone Links feature is installed and operational on your system.

5.1 Managing the Routers, Gateways, and Backhaul Switches

Routine operational procedures for Flexible Site and InterZone Links involve the following:

- Backups of router, gateway, and switch configuration files
- Verification and compliance audits of router, gateway, and switch configuration files

See the *Unified Network Configurator* manual for details.

This page intentionally left blank.

Chapter 6

Troubleshooting

This chapter covers fault management for the Flexible Site and InterZone Links feature.

6.1 Ethernet Links – Fault Management

The following table describes troubleshooting scenarios and tips relating to an implementation of the Flexible Site and InterZone Links.

Table 4: Flexible Site and InterZone Links – Troubleshooting

Problem	Troubleshooting Steps
Lack of connectivity in a site or zone (for example, site dropping wide area functionality and going into site trunking mode)	**1** Check the status of the affected devices and links in the Unified Event Manager (UEM). **2** If all devices on the affected network path are operating normally, test the Ethernet link at the site for connectivity if possible, or contact the service provider to determine if the backhaul link is down.
Impaired audio quality and truncation experienced by radio or console users	**1** Check with the service provider to determine if there are problems with backhaul network performance (for example, severe network congestion that may result in a long queue of packets waiting to be transmitted). **2** Contact the Motorola Solutions Support Center (SSC) for further assistance in diagnosing the problem.

6.2 Ethernet Links – Troubleshooting Tools

The Unified Event Manager (UEM) provides tools for troubleshooting Ethernet links.

6.2.1 Unified Event Manager (UEM) for Ethernet Link Troubleshooting

The Unified Event Manager (UEM) fault management application provides the functionality to assist in identifying network problems associated with Flexible Site and InterZone Links.

The UEM displays the link Up, link Down, link Disabled, and link Degraded states reported by the routers or gateways at the Ethernet link endpoints. The Degraded state indicates that the configurable threshold for a specific statistic (delay, jitter, or packet loss rate) has been exceeded for that reporting interval.

The UEM displays events received from routers or gateways when links become degraded, based on user configurable action limits. This information is useful in identifying the general location of the problem on the network path through which communication occurs – Zone Core out to the Ethernet backbone, remote site out to the Ethernet backbone, and so on.

The UEM also may display events from routers or gateways to indicate that the packet queues in the devices are exceeding the design specifications (QueueDepthCaution, QueueDepthExceeded, TotalQueueDepthExceeded). If these events are observed in the UEM, it is typically due to a misconfiguration of the backhaul bandwidth parameters.

Network devices must be discovered in the UEM. This is done by initiating a subnet or node (IP-based) device discovery action for the status to be viewable in the UEM. See the *Unified Event Manager* manual for details.

6.2.1.1 Ethernet Link Statistics in the UEM

Ethernet link statistics polling is a configurable option in the Unified Event Manager (UEM). These statistics are collected from the Motorola Network Routers and GGM 8000 gateways, and are used for network performance analysis.

The UEM performs the following functions:

- Collects Ethernet link performance statistics from the network transport subsystem for each Ethernet link endpoint of the system. Collection occurs once per statistics publication interval. The polling interval is set to 15 minutes by default, but is configurable at runtime for intervals of up to 1 hour.
- Retains all the system Ethernet link performance statistics for at least one week.
- Displays stored Ethernet link performance statistics in a table format.
- Displays Ethernet link performance statistics in statistics values versus time graphs.

For each measurement interval, at each end of every Ethernet WAN link, the Network Management subsystem provides the following details:

- Average, minimum, and maximum value of the round-trip IP Packet Transfer Delay (IPTD)
- Average of the one-way IP Packet Delay Variation (IPDV)
- Average 99th-percentile value of the one-way IPDV
- IP Packet Loss Rate (IPLR)

NOTICE: All of these statistics are enabled by default in the UEM. They are collected for all routers and gateways in the system and are displayed in the UEM even for routers and gateways that do not have Ethernet WAN interfaces configured. In such a case though, there is no data available for the statistics.

6.2.1.2 Ethernet Link Statistics Configured for Data Collection

Table 5: Ethernet Link Statistics Configured for Data Collection

Statistic Name	Description
Ethernet WAN IF: IPTD Number	Number of successful round-trip IPTD measurements for last interval.
Ethernet WAN IF: IPTD Sum	Sum of the round-trip IPTD measurements for last interval.
Ethernet WAN IF: IPTD Average (enabled by default)	Average value of the round-trip IPTD measurements for last interval.
Ethernet WAN IF: IPTD Sum Squares	Sum of squares of the round-trip IPTD measurements.

Table continued…

Statistic Name	Description
Ethernet WAN IF: IPTD Maximum (enabled by default)	Maximum round-trip IPTD measurement for last interval.
Ethernet WAN IF: IPTD Minimum (enabled by default)	Minimum round-trip IPTD measurement for last interval.
Ethernet WAN IF: IPDV Number	Number of successful IPDV measurements for last interval.
Ethernet WAN IF: IPDV Sum	Sum of the IPDV measurements for last interval.
Ethernet WAN IF: IPDV Average (enabled by default)	Average value of the IPDV measurements for last interval.
Ethernet WAN IF: IPDV Sum Squares	Sum of squares of the IPDV measurements for last interval.
Ethernet WAN IF: IPDV 99% Number	Number of successful measurements of the 99th percentile IPDV for last interval.
Ethernet WAN IF: IPDV 99% Sum	Sum of the measurements of the 99th percentile IPDV for last interval.
Ethernet WAN IF: IPDV 99% Average (enabled by default)	Average value of the 99th percentile IPDV measurements for last interval.
Ethernet WAN IF: IPDV 99% Maximum	Maximum 99th percentile IPDV measurements for last interval.
Ethernet WAN IF: IPDV 99% Minimum	Minimum 99th percentile IPDV measurements for last interval.
Ethernet WAN IF: IPLR Tx Packet Number	Number of packets transmitted by the source endpoint in successful IPLR measurement attempts for last interval.
Ethernet WAN IF: IPLR Packet Not Received	Number of packets that were not received by the receiving endpoint for last interval.
Ethernet WAN IF: IPLR Loss Rate (enabled by default)	IP packet loss rate (that is, number of packets not received divided by number of packets transmitted) for last interval.

6.3
Audio Quality Troubleshooting

If audio quality or truncation issues occur, a fundamental troubleshooting approach is to ensure that link delay, jitter, and packet loss conditions are maintained within appropriate specifications. Routers and gateways that support Flexible Site and InterZone Links can store performance-monitoring statistics for link delay, jitter, and packet loss rates. These statistics can be used to analyze and explain possible audio quality and truncation issues. This information is available through the Unified Event Manager or InfoVista.

NOTICE: Some devices in the system support a configurable jitter buffer. If audio quality problems are experienced on backhaul networks with excessive jitter, it may be possible to adjust the jitter buffer for some devices. Although it is possible to configure the jitter buffers manually, it is not recommended, as it might cause serious performance issues. If you wish to adjust jitter buffers, contact the Motorola Solutions Customer Service Center for detailed instructions.

6.4 Fault and Performance Management

The states of the Flexible Site and InterZone Links encapsulation endpoints are monitored from the Unified Event Manager (UEM). The valid states are Up, Down, Disabled, and Degraded. The following configurable thresholds (statistics) determine the state of the Flexible Site and InterZone Links object:

- Link Delay
- Packet Loss
- Jitter

A default measurement interval of 15 minutes is used to evaluate whether these thresholds are exceeded. If the measurement interval passes with all three statistics below the threshold, the Flexible Site and InterZone Links object is in the Up state. If the configurable threshold statistic for any of the three is exceeded for the measurement interval (the default is 15 minutes), the Ethernet Site and InterZone Links object reports a Degraded state. The state transitions to Down when the link is down or it is set to Disabled when a value of “0” is set for any threshold.

The following default thresholds are applied:

- Threshold 99th Percentile Jitter (IPDV) = 10 ms (range = 1 ms to 200 ms)
- Threshold Packet Loss Rate (IPLR) = 0.02% (range = 0.01% to 2% in 0.01% increments)
- Threshold Round Trip Delay (IPTD) = 40 ms(range = 10 to 1000 ms in 1 ms increments)

NOTICE: For a geographically intra-prime site link, the following default threshold is used:

- IPDV Avg99Percent = 4 ms
- IPLR PktRate = 0.02%
- IPTD AvgRtXfer = 15 ms

These thresholds can be modified, but if any of the actual Flexible Site and InterZone Links exceeds the thresholds, alarms and events continue to be generated until the thresholds are modified in the Unified Network Configurator (UNC). See "Chapter 4, UNC Saved Commands and Templates" in the *Unified Network Configurator* manual to modify the thresholds. With the use of the UNC, statistical thresholds are set for the core router, core gateway, exit router, prime site access router, site router, and site gateway objects. The modifications required to set these statistical thresholds depend on your system architecture (such as single site links and dual site links). Routers and gateways that support Flexible Site and InterZone Links (IPv4 or IPv6) implement performance monitoring across the backhaul network. It includes monitoring link latency, jitter, and packet loss.

Link statistic alarms and events are reported to the UEM. The maximum link delay, jitter, and packet loss rate for each link is required to support pre-configuration of the ASTRO® 25 system trap thresholds. See the *Unified Event Manager* manual for more details.

If audio quality or truncation issues are experienced, the fundamental troubleshooting step is to ensure that the delay, jitter, and packet loss budgets for the backhaul network are within specifications. This information is available through the UEM or InfoVista for up to one week in the table, graph, or as a CSV file.

IMPORTANT: If you obtain delay, jitter, and packet loss statistics from the backhaul service provider, it is imperative to understand the techniques used to measure them. The statistics reported in the UEM and InfoVista are defined as follows:

- Latency, or IP Packet Transfer Delay, is defined per RFC 2861.
- Jitter statistics are specifically 99th percentile jitter per ITU Recommendation Y.1541. Jitter is **not** reported as an average.
- Packet loss refers to **Type-P-One-Way-Packet-Loss**, as defined in RFC2680, section 2.4. In the context of audio for the ASTRO® 25 system, reordered packets are also considered packet loss.

Troubleshooting site links is enhanced using these statistical threshold alarms and events for Ethernet site links. If alarms and events are encountered for Flexible Site and InterZone Links on a newly or recently upgraded system, the issue may be related to default values that do not match the expected backhaul link characteristics. If alarms and events are encountered for Flexible Site and InterZone Links that have been in service for some time, then the issue is most probably related to the degradation in service on your backhaul links. In this case, contact your service provider. Any troubleshooting for Flexible Site and InterZone Links performance issues requires good record keeping and documentation of the expected backhaul link performance characteristics along with an understanding of the Service Level Agreement with your service provider.

This page intentionally left blank.

Chapter 7

FRU/FRE Information

This chapter lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) and references replacement procedures applicable to the Flexible Site and InterZone Links feature.

7.1

Field Replaceable Unit (FRU)

There is one Field Replaceable Unit (FRU) available for the Flexible Site and InterZone Links feature. Use the part number for the item when ordering.

Table 6: Flexible Site and InterZone Links FRU

Field Replaceable Unit (FRU)	Motorola Solutions Part Number
S2500 10Base-T Ethernet Module	ST2510

For the S2500 router Ethernet module replacement procedure, see the *System Routers – S6000/S2500* manual.

7.2

Field Replaceable Entities (FREs)

The following table contains the Field Replaceable Entities (FREs) available for the Flexible Site and InterZone Links. Use the part number for the item when ordering.

For S2500 and S6000 router replacement procedure, see the *S6000 and S2500 System Routers* manual. For the GGM 8000 gateway replacement procedure, see the *GGM 8000 System Gateways* manual.

Table 7: Flexible Site and InterZone Links FREs

Field Replaceable Entity (FRE)	Part Number
HP ProCurve 2620–24 LAN Switch (for core and prime site backhaul switches)	CLN1856A
Extreme Networks E4G 200 Cell Site Router (for core and prime site backhaul switches in Layer 2 networks)	Contact Cambium Networks for details.
Extreme Networks E4G 400 Cell Site Router (for core and prime site backhaul switches in Layer 2 networks)	Contact Cambium Networks for details.
S2500 router	ST2500
S6000 router	ST6000
GGM 8000 gateway **NOTICE:** Together with an appropriate power supply: TPN6210A (AC power supply) TPN6211A (DC power supply).	TYN4001A or TYN4001B (new base module)

This page intentionally left blank.

Chapter 8

Ethernet Site Links – Expansion

This chapter supports the Ethernet Site Link Expansion process with Ethernet Site Link Expansion procedures.

NOTICE: Depending on the transport devices used in your system, the site routers or transport devices mentioned in this chapter would be either a Site Gateway (GGM 8000 platform) or the S6000/S2500 platform.

8.1

Ethernet Site Links – Expansion

Follow the procedures for converting hardware while expanding Ethernet Site Links.

The S2500 router does not support IPv6. If you are converting T1 links or IPv4 links to IPv6, first replace the S2500 router with a GGM 8000 gateway.

When a GGM 8000 replaces an S2500, you may need to add an encryption module , depending on where the replacement device was sourced from:

- If the GGM 8000, with the encryption option enabled, is sourced from the factory, it has the necessary certificate to perform encryption and does not need an encryption module added.
- If the GGM 8000 comes from a different source, an encryption module must be added.

Process:

1

If…	Then…
If you want to maintain core router redundancy during conversion,	see Site Link Conversion While Maintaining Core Router Redundancy on page 67.
Otherwise,	continue with step 3.

2 Convert even-numbered core routers.

See Converting Core Routers on page 67.

3 Convert site routers.

If…	Then…
If this is a single link site, and you want to minimize downtime,	see Converting Site Routers – Ethernet Site Link Expansion – Single Link, Spare Router on page 65 **NOTICE:** If the site router is an S2500, a spare router is not required to minimize the downtime since a replacement router for S2500 with a GGM 8000 is required and is provided.
If this is a single link site, and some downtime is acceptable,	see Converting Site Routers – Ethernet Site Link Expansion – Single Link, Existing Router on page 64.

If…	Then…
If this is a dual link site,	see Converting Site Routers – Ethernet Site Link Expansion – Dual Link, Existing Routers on page 66.

4 Convert odd-numbered core routers.

See Converting Core Routers on page 67.

5 Perform InterZone link conversion.

See InterZone Link Conversion on page 68.

6 Perform CEN link conversion. See CEN Link Conversion on page 69.

7 Perform backhaul switch configuration.

The backhaul switch configuration to support Ethernet Site Links can be found in the *System LAN Switches* manual.

8.1.1 Converting Site Routers – Ethernet Site Link Expansion – Single Link, Existing Router

When and where to use:
The process for Ethernet Site Link Expansion depends on the site type and the use of existing or spare routers.

Procedure:

1 In a T1 to IPv6 or a IPv4 to IPv6 conversion on an S6000 router, if the encryption module is not present, add the encryption module to the router and load IPv6 PSKs on the router. For details on adding the PSKs, see the “Adding a Pre-Shared Key for Link Encryption” section in the *Link Encryption and Authentication* manual.

2 Log on to the UNC from the NM client. See the “Logging On to the EMC Smarts Network Configuration Manager” procedure in the *Unified Network Configurator* manual.

3 Use the UNC to download configuration to the device. See the “Updating OS and Configuration Files on MNRs and Switches in UNC” procedure in the *Unified Network Configurator* manual.

4 If this is a Simulcast Prime site, install the Ethernet backhaul switch.

If…	Then…
If this is an S6000 router,	connect port 3 on the site router.
If this is a GGM 8000 gateway,	connect port 3 on the site gateway.

5 Reboot the site router/gateway.

NOTICE: Downtime – the site link goes down and the site goes into the site trunking until the router reboots.

6 If Link Encryption is enabled, enter encryption keys on both transport devices (site gateways or routers) at both ends of each link.

7 Verify that the site link has come back up. Test for wide area call capability.

8 Log on to the UEM. See the “Starting the UEM Client” procedure in the *Unified Event Manager* manual.

9 Rediscover the device in the UEM. See the “Discovering Devices” procedure in the *Unified Event Manager* manual.

10 Log on to the UNC from the NM client. See the “Logging On to the EMC Smarts Network Configuration Manager” procedure in the *Unified Network Configurator* manual.

11 Update the UNC by making it rediscover the new site router. See “Performing Device Discovery with the UNCW Discovery Wizard” procedure in the *Unified Network Configurator* manual.

8.1.2

Converting Site Routers – Ethernet Site Link Expansion – Single Link, Spare Router

Prerequisites:
In a T1 to IPv6 or a IPv4 to IPv6 conversion, prepare a spare site router/gateway with an Ethernet WAN interface hardware module and IPv6 Ethernet WAN configuration.

NOTICE: In a S2500 device, a spare router is not required to minimize the downtime, since a replacement router for S2500 with a GGM 8000 is required and will be provided.

Procedure:

1 If MAC Port Lockdown is enabled on the site switch, disable it in the UNC.

2 If this is a Simulcast Prime Site, install the Ethernet backhaul switch.

3 Disconnect the original site router from the site’s WAN link and from the site’s Ethernet switch.

NOTICE: The site link goes down, and the site goes into site trunking until the site link is restored.

If…	Then…
If this is an S6000 router,	connect port 3 on the site router.
If this is a GGM 8000 gateway,	connect port 3 on the site gateway.

4 If Link Encryption is enabled, enter encryption keys in both transport devices (site gateway or routers) at both ends of each link.

5 Verify that the site link has come back up. Test for wide area call capability.

6 If MAC Port Lockdown was disabled on the site switch, enable it in the UNC.

7 Log on to the UEM. See the “Starting the UEM Client” procedure in the *Unified Event Manager* manual.

8 Rediscover the device in the UEM. See the “Discovering Devices” procedure in the *Unified Event Manager* manual.

9 Log on to the UNC from the NM client. See the “Logging On to the EMC Smarts Network Configuration Manager” procedure in the *Unified Network Configurator* manual.

10 Update the UNC by making it rediscover the new site router. See the “Performing Device Discovery with the UNCW Discovery Wizard” procedure in the *Unified Network Configurator* manual.

8.1.3

Converting Site Routers – Ethernet Site Link Expansion – Dual Link, Existing Routers

Procedure:

1 Log on to the UNC from the NM client. See the “Logging On to the EMC Smarts Network Configuration Manager” procedure in the *Unified Network Configurator* manual.

2 Use the UNC to download configuration to the device. See the “Updating OS and Configuration Files on MNRs and Switches in UNC” procedure in the *Unified Network Configurator* manual.

3 If this is a Simulcast Prime Site, install the Ethernet backhaul switch.

4 In a T1 to IPv6 or a IPv4 to IPv6 conversion, for encrypted Ethernet Site Links, add an encryption module to the router and load IPv6 Pre-Shared Keys on the router.

5 Disconnect the site WAN link (site gateway or site router) and its link from the site Ethernet switch.

6 Prepare the secondary site router’s hardware for Ethernet WAN connection by removing its T1 interface module and inserting a second Ethernet interface module.

If…	Then…
If this is an S2500 router,	connect port 2 on the site router (S2500) to the appropriate port on the Ethernet backhaul service provider’s device (this may be a switch or a router). Ensure that the backhaul device is configured for 10/Full, as this is the only speed/duplex setting supported on the S2500.
If this is an S6000 router,	connect port 3 on the site router.
If this is a GGM8000 gateway,	connect port 3 on the site gateway.

7 Power up the site router/gateway.

8 If Link Encryption is enabled, enter encryption keys in both transport devices (site gateway or routers) at both ends of each link.

9 Verify that the site link has come back up.

10 Log on to the UEM. See the “Starting the UEM Client” procedure in the *Unified Event Manager* manual.

11 Rediscover the device in the UEM. See the “Discovering Devices” procedure in the *Unified Event Manager* manual.

12 Log on to the UNC from the NM client. Follow the “Logging On to the EMC Smarts Network Configuration Manager” procedure in the *Unified Network Configurator* manual.

13 Update the UNC by making it rediscover the new site router/gateway. See the “Performing Device Discovery with the UNCW Discovery Wizard” procedure in the *Unified Network Configurator* manual.

14 The primary site router/gateway is converted by repeating the steps above.

8.1.4 Converting Core Routers

Procedure:

1. In a T1 to IPv6 or a IPv4 to IPv6 conversion on an GGM 8000 gateway router, if the encryption module is not present, add the encryption module to the router and load IPv6 PSKs on the router. For details on adding the PSKs, see the “Adding a Pre-Shared Key for Link Encryption” section in the *Link Encryption and Authentication* manual.
2. Log on to the UNC from the NM client. See the “Logging On to the EMC Smarts Network Configuration Manager” procedure in the *Unified Network Configurator* manual.
3. Use the UNC to download configuration to the device. See the “Updating OS and Configuration Files on MNRs and Switches in UNC” procedure in the *Unified Network Configurator* manual.
4. Install the Ethernet backhaul switch.
5. Connect port 3 on the Core routers to the appropriate port on the Ethernet backhaul switch.
6. Reboot the Core routers.
7. Verify connectivity to sites, using the ping command and the LAN address of the sites.
8. Log on to the UEM. See the “Starting the UEM Client” procedure in the *Unified Event Manager* manual.
9. Rediscover the devices in the UEM. See the “Discovering Devices” procedure in the *Unified Event Manager* manual.

8.1.5 Site Link Conversion While Maintaining Core Router Redundancy

Procedure:

1. Install the additional core router pair (core 7 and core 8) in the zone.
2. If MAC Port Lockdown is enabled on the core LAN switch, disable it for core 7 and core 8 ports, in the UNC.
3. Modify the configuration for core router 1 to disable the following events, by adding a # in front of the command.

   ```
   #ADD !eth1 -SCH EbmeEVent PortUp 20000 do tlanUp eth1 dualpathsite
   #ADD !eth2 -SCH EbmeEVent PortUp 20000 do tlanUp eth2 dualpathsite
   ```

4. Modify the configuration for core router 2 to disable the virtual interfaces for the Ethernet site links, by appending the following command for each port at the end of the `boot.cfg` file.

   ```
   SETDefault !v<ZZZ> -POrt CONTrol = Disable
   ```

   NOTICE: ***<ZZZ>*** is the virtual interface of the Ethernet site link.

5. Push down the modified configuration to the routers manually, using TFTP.
6. Reboot the routers to activate the new `boot.cfg` configurations.
7. Use the following procedures to upgrade the sites:
   - Converting Site Routers – Ethernet Site Link Expansion – Single Link, Existing Router on page 64
   - Converting Site Routers – Ethernet Site Link Expansion – Single Link, Spare Router on page 65

- Converting Site Routers – Ethernet Site Link Expansion – Dual Link, Existing Routers on page 66

8 If Link Encryption is enabled, enter encryption keys in both transport devices (site gateway or routers), at both ends of each link.

9 Use VoyenceControl to enable the virtual ports for the Ethernet site links by sending the following command and appending it to the `boot.cfg` file on core routers 7 and 8:

```
SETDefault !v<ZZZ> -POrt CONTrol=enable
```

NOTICE: ***<ZZZ>*** is the virtual interface of the Ethernet site link.
The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

10 Coordinate and repeat step 7and step 8 for each Ethernet site link.

11 When the last site is complete, push down the original configuration for the Ethernet site links to core router 1 and 2.

12 Power down core router 8, and reboot core router 2.

13 Once core router 2 is up, power down core router 7, and reboot core router 1.

14 Re-discover core router 1 and 2 in the UEM and the UNC.

See the “Updating OS and Configuration Files on MNRs and Switches in UNC” procedure in the *Unified Network Configurator* manual.

8.1.6
InterZone Link Conversion

Procedure:

1 Disconnect the inactive CWR exit router in each zone from its InterZone WAN link (this should be the exit router 2).

2 Connect exit router 2 in each zone to the Ethernet WAN transport.

If…	Then…
Optional: If this is a T1 to IPv4 conversion (for systems with encryption),	load IPv4 Pre-Shared Keys on the router.
If this is a T1 to IPv6 conversion or an IPv4 to IPv6 conversion,	add the encryption module, if it is not present, to the router, and load IPv6 PSKs on the router. For details on adding the PSKs, see the “Adding a Pre-Shared Key for Link Encryption” section in the *Link Encryption and Authentication* manual.

3 Use the UNC to download the Ethernet Site link configuration to exit router 2 in each zone.

See the “Updating OS and Configuration Files on MNRs and Switches in UNC” procedure in the *Unified Network Configurator* manual.

4 Reboot exit router 2 in each zone.

5 If Link Encryption is enabled, enter encryption keys in both transport devices (site gateway or routers), at both ends of each link.

6 Repeat step 1 to step 5 for exit router 1 in each zone.

7 Re-discover exit router 1 and 2 in each zone with the UEM and the UNC.

See the “Updating OS and Configuration Files on MNRs and Switches in UNC” procedure in the *Unified Network Configurator* manual.

8.2 CEN Link Conversion

This section addresses the case where a Customer Enterprise Network (CEN) interface (located remotely from a zone core) is being converted to Ethernet WAN. It applies to Fortinet Firewall.

Procedure:

1. Load the RNI-DMZ firewall, DMZ switch, and the Border Router with their Ethernet WAN configuration (but do not activate it yet).
2. Connect the DMZ switch and the Border Router to the Ethernet WAN transport.

If…	Then…
Optional: If this is a T1 to IPv4 conversion (for systems with encryption),	load IPv4 Pre-Shared Key on the Border Router and the RNI-DMZ Firewall.
If this is a T1 to IPv6 conversion or an IPv4 to IPv6 conversion (for Fortinet firewall),	perform the following actions: **a** Load the IP configuration report file into UEM, see: *Unified Event Manager* manual. **b** Add an encryption module (if it is not present) to the router, and load IPv6 Pre-Shared Keys on the Border Router and the RNI-DMZ Firewall.

3. Activate the RNI-DMZ Firewall, the DMZ switch, and the Border Router with their Ethernet WAN configuration.

   ⚠ **WARNING:** Data services that rely on this CEN connection are unavailable from the time these routers are rebooted until their Ethernet WAN link comes up.

4. Verify that the Ethernet WAN link between the firewall and the border router has come up.
5. Verify CEN application traffic flow between the CEN and the Master Site.

This page intentionally left blank.