555-8421-210

Meridian Internet Gateway

Reach Line Card

Installation and Administration Guide

Product release 1.0 Standard 1.0 March 2000

NORTEL NETWORKS™

How the world shares ideas.

NTDR82AA

Meridian Internet Gateway

Reach Line Card

Installation and Administration Guide

Product release:	1.0
Publication number:	555-8421-210
Document release:	Standard 1.0
Date:	March 2000

Printed in the United States of America

All information contained in this document is subject to change without notice. Nortel Networks reserves the right to make changes to equipment design or program components, as progress in engineering, manufacturing methods, or other circumstances may warrant.

Publication history

March 2000	This is the Standard 1.0 issue of the *Meridian Internet Gateway Reach Line Card Installation and Administration Guide*.

Contents

Preface

About this document

In this preface

Overview

Welcome

Nortel Networks is pleased to announce the Meridian Internet Gateway Reach Line Card (MIG RLC).

A standard MIG RLC works with multiple remoting solutions to provide Meridian 1 PBX service to telephones at one or more remote sites any distance from the host PBX. The MIG RLC is compatible with Remote Office 9150 sites.

Introduction

The *Meridian Internet Gateway Reach Line Card Installation and Administration Guide* provides information on how to configure and maintain your MIG RLC.

A MIG RLC requires no external components at the host Meridian 1 PBX location. Simply install the MIG RLC in place of a standard Nortel Networks extended digital line card (XDLC), and configure it through the Meridian 1 database as if it serves locally connected telephones.

You can use channels that are not needed for remote telephones for local telephones so that all channels of the MIG RLC provide service to your corporate telecommunications network.

For information on other tools and features of the remoting product served by your MIG RLC, refer to the documentation specific to that product. A list of documents that relate to other elements of the Remote Office system is included on page xix.

Who should read this guide

This guide is for telecom and data network managers and administrators who plan, install, and manage corporate telecommunications and data networks on a daily basis.

Assumptions

It is assumed that individuals who use this guide are familiar with the following subjects:

- basic telecommunications terminology
- PC terminology and operation (specifically Windows 95, Windows 98, or Windows NT 4.0)
- Nortel Networks PBX terminology, functionality, and administration

About this guide

Introduction

This guide contains the following information:

- detailed descriptions of the MIG RLC and the procedures necessary to properly install and configure it
- required configuration of the Meridian 1 switch into which the line card is placed
- procedures for administering the line card after installation
- testing procedures to aid in administration
- suggested troubleshooting procedures for addressing possible problems

How to use this guide

This guide provides step-by-step procedures for installing, configuring, and using the MIG RLC with your Nortel Networks remoting product. Review this guide before you install and configure your MIG RLC.

When you are ready to begin, follow the steps for planning, installing, and configuring your hardware in the order in which they are presented in this guide. This helps you to achieve a successful, trouble-free installation.

In this guide

Chapter 1, “Meridian Internet Gateway Reach Line Card description”
This chapter provides a thorough description of the MIG RLC, including its physical architecture, features, configuration, connection options, and operation.

Chapter 2, “Planning for installation”
This chapter outlines the preparation that is crucial to integrating the MIG RLC into your existing corporate data and telecommunications networks.

Chapter 3, “Installing the Meridian Internet Gateway Reach Line Card”
This chapter discusses the procedures necessary to install and cable the MIG RLC on your Meridian 1 PBX.

Chapter 4, “Configuring the PBX for the Meridian Internet Gateway Reach Line Card”
This chapter contains information necessary for configuring the Meridian 1 PBX to communicate properly with the MIG RLC.

Chapter 5, “Configuration Manager overview”
This chapter describes the Configuration Manager, the software application used to configure and administer the MIG RLC.

Chapter 6, “Configuring the Meridian Internet Gateway Reach Line Card”
This chapter explains how to configure the MIG RLC so that it can communicate with the remote units to which it is connected.

Chapter 7, “Administration”
This chapter provides procedures for administering the MIG RLC.

Chapter 8, “Troubleshooting”
This chapter provides steps you can take to troubleshoot a few problems you might face with the MIG RLC.

Appendix A, “Network engineering guidelines”
This appendix provides guidelines for evaluating and setting Quality of Service on your IP network. If you install the Remote Office product in your IP network without performing the preliminary assessments that are described, this can result in unacceptable degradation in voice service to users.

Appendix B, “Planning forms”
This appendix provides sample forms to help you

- plan the MIG RLC configuration
- determine what you need to expand the MIG RLC’s voice processing capabilities

Appendix C, “Sample configuration files”
This appendix provides the following:

- a sample network diagram that shows one host site (MIG RLC installed on the host PBX) and one Remote Office 9150 unit (with one user station)
- sample configurations using information from the network diagram

The purpose of this appendix is to demonstrate the relationship between configuration settings on each unit in the network.

Appendix D, “Pin-out tables for RLC Multi-I/O cables”
This appendix provides pin-out tables for the RLC Multi-I/O cable–Basic and RLC Multi-I/O cable–Enhanced.

Appendix E, “Safety and regulatory information”
The MIG RLC complies with a variety of regulatory standards and classifications. You can find details concerning the safety and regulatory classifications earned by the MIG RLC in this appendix.

Glossary
Many terms in this manual have meanings specific to the telecommunications and data networking fields, or specific to the MIG RLC. The glossary contains definitions of terms used in this manual, as well as a few related terms.

Indexes
Use the fields index when you want to know the function of a specific Configuration Manager field.

The main index provides an alternate method of locating information in this guide.

Skills you need

Introduction

This section describes the skills and knowledge you need to use this guide effectively.

Nortel Networks product knowledge

Knowledge of, or experience with, the following Nortel Networks products and concepts is helpful when working with the MIG RLC:

- basic administration of the Meridian 1 switch (telephone set and XDLC configuration)
- characteristics and principles of XDLC operation

Telecommunications knowledge

Knowledge of, or experience with, the following aspects of telecommunications is helpful when working with the MIG RLC:

- digital telephone configuration
- ISDN PRI configuration
- trunk configuration
- switch configuration
- fundamental data networking
- switch maintenance (SDI operation)

Data networking knowledge

Knowledge of, or experience with, the following aspects of data networking is helpful when working with the MIG RLC:

- the following aspects of data link (Layer 3 of the OSI model)
  - IP protocol
  - routing

- network addressing
- network traffic analysis and provisioning
- network configuration
- Voice over IP concepts

PC knowledge

The knowledge of, or experience with, the following PC products as appropriate for your network is helpful when administering the MIG RLC:

- general knowledge of Microsoft Windows
- software installation
- network configuration

Other experience or knowledge

Other types of experience or knowledge that are helpful include the following:

- knowledge of RS-232 signaling
- analytical skills
- troubleshooting skills

Related information products

Introduction

This section lists documents and CD-ROMs in which you can find additional information related to the MIG RLC.

Printed documents

Remote Office and MIG RLC Release Notes (NTP 555-8421-102)

This document describes the features and known problems for the MIG RLC and Remote Office 9150 branch office system.

Note: The printed copy might supersede the copy provided on the CD-ROM. You can obtain the most up-to-date version of all printed documents on the Nortel Networks web site. For download instructions, see “How to obtain the documentation and CD-ROMs” on page xx.

Remote Office 9150 Installation and Administration Guide (NTP 555-8421-210)

This document describes how to install, configure, and manage the Remote Office 9150 unit.

Installer’s Notes

The following Installer’s Notes are quick reference documents that are provided with the component discussed in the document:

- *Meridian Internet Gateway Reach Line Card Installer’s Notes*
- *Remote Office 9150 and MIG RLC DSP Module Installer’s Notes*
- *Remote Office 9150 Trunk Interface Module Installer’s Notes*

Each document summarizes the installation and configuration procedures for the component and provides cross-references to other documents for more detailed information.

Note: You cannot order these documents separately.

CD-ROMs

The following CD-ROMs are available for the MIG RLC:

- *Remote Office Product CD-ROM*

  The Product CD-ROM contains the following:

  - documentation in Adobe Acrobat Reader (PDF) format
  - firmware
  - Configuration Manager software

- *Remote Office Technical Training Course 100 CD-ROM*

  The Technical Training CD-ROM contains a web-based course for Nortel Networks distributors and the administrators of Nortel Networks customers. The web-based course explains how to install, configure, and manage the MIG RLC.

How to obtain the documentation and CD-ROMs

You can order the printed documentation and CD-ROMs from your Nortel Networks distributor.

You can also download the documentation in Adobe Acrobat Reader (PDF) format from the Nortel Networks web site at http://www.nortelnetworks.com/remoteoffice. For more information, refer to *Remote Office and MIG RLC Release Notes* (NTP 555-8421-102).

Conventions used in this guide

Introduction

This section describes the conventions used in this guide.

Precautionary messages

Note: A note describes the secondary results of procedures or commands, or special conditions under which you must use a procedure or command.

ATTENTION

Provides information essential to the completion of a task.

CAUTION

Risk of data loss or equipment damage
Cautions you against unsafe practices or potential hazards, such as equipment damage, service interruption, or loss of data.

WARNING

Risk of minor personal injury
Warns you of a potentially hazardous situation that can result in minor or moderate injury.

DANGER

Risk of death or serious personal injury
Alerts you to an immediate hazard that can result in death or serious injury.

DANGER

Risk of electric shock
Alerts you to an immediate hazard that can result in death or serious injury through high voltage or electric shock.

How this guide presents instructions for selecting menu options

To simplify the instructions for selecting menu options, this guide abbreviates the selection path. For example, if you must choose Over IP from the Remote Connectivity menu, which is under the Tests menu, this guide uses the following style:

From the menu, choose Tests → Remote Connectivity → Over IP.

How this guide presents instructions for displaying property sheets

To simplify the procedures for accessing property sheets, this guide summarizes instructions in “Getting there” statements.

The procedure for displaying the screen that you need depends on whether you are

- performing an online configuration (that is, you are connected to a node by serial port or Telnet)
- performing an offline configuration (that is, you are not connected to a node)

The short, “Getting there” instruction appears in the following format:

Getting there 9150 → Configuration Manager → IP Configuration

The long instruction for this example is shown on the next page.

1 Do the following:

IF	THEN
you are performing an offline configuration	select the device type as described in "To select the device type" on page 135.
you are performing an online configuration	connect to, then log on to the node as described in "Logging on to a unit" on page 111.

2 In the left pane, click the plus sign beside Configuration Manager to expand the node list.

3 Click IP Configuration.

Result: The IP Configuration property sheet for the MIG RLC appears in the right pane.

Chapter 1

Meridian Internet Gateway Reach Line Card description

In this chapter

Overview

Introduction

This chapter provides a thorough description of the Meridian Internet Gateway Reach Line Card (MIG RLC), including its physical architecture, features, configuration, connection options, and operation.

Physical features

Certain elements of the MIG RLC enable you to perform maintenance activities, such as

- monitoring the basic health of your MIG RLC
- expanding the number of ports your MIG RLC can support
- linking the MIG RLC to other elements of your remoting system

Operational characteristics

The MIG RLC provides a number of unique features that distinguish it from other remoting products.

These features include

- Nortel Networks' patented Quality of Service (QoS) transitioning technology
- variable security
- packet voice processing
- dial-up trunking
- transparent operation
- Meridian telephone equipment compatibility

Physical features

Introduction

Certain elements of the MIG RLC enable you to perform card maintenance activities. These elements and associated maintenance activities include

- LED indicators that enable you to monitor your MIG RLC's basic health and Ethernet traffic
- DSP expansion modules that enable you to increase the number of simultaneously active remote ports supported by your MIG RLC
- cabling connections that enable you to link your MIG RLC with other elements of your Remote Office

The Meridian Internet Gateway Reach Line Card

The 16-channel version of the MIG RLC (NTDR68xx) is a single-wide line card that provides service for up to 16 telephones. At the host location, install the 16-channel version of the MIG RLC in an IPE shelf or Option 11 cabinet of a Meridian 1 PBX to provide service for up to 16 telephones.

The double-wide, 32-channel version of the MIG RLC (NTDR70xx or NTDR71xx) provides service for up to 32 telephones.

The MIG RLC emulates a standard digital line card (XDLC), providing PBX functionality for telephones at remote locations. The MIG RLC supports the Remote Office 9150 unit.

Configure each port on the MIG RLC from the Meridian 1 database as if telephones were locally connected to a standard digital line card (XDLC). Your existing Meridian digital trunks (ISDN PRI) and an integrated 10BaseT Ethernet interface (Voice over IP) carry the voice and signaling traffic as packets.

You can upload MIG RLC firmware through a customer-provided Trivial File Transfer Protocol (TFTP) server installed on the administration PC, through a 10BaseT Ethernet connection.

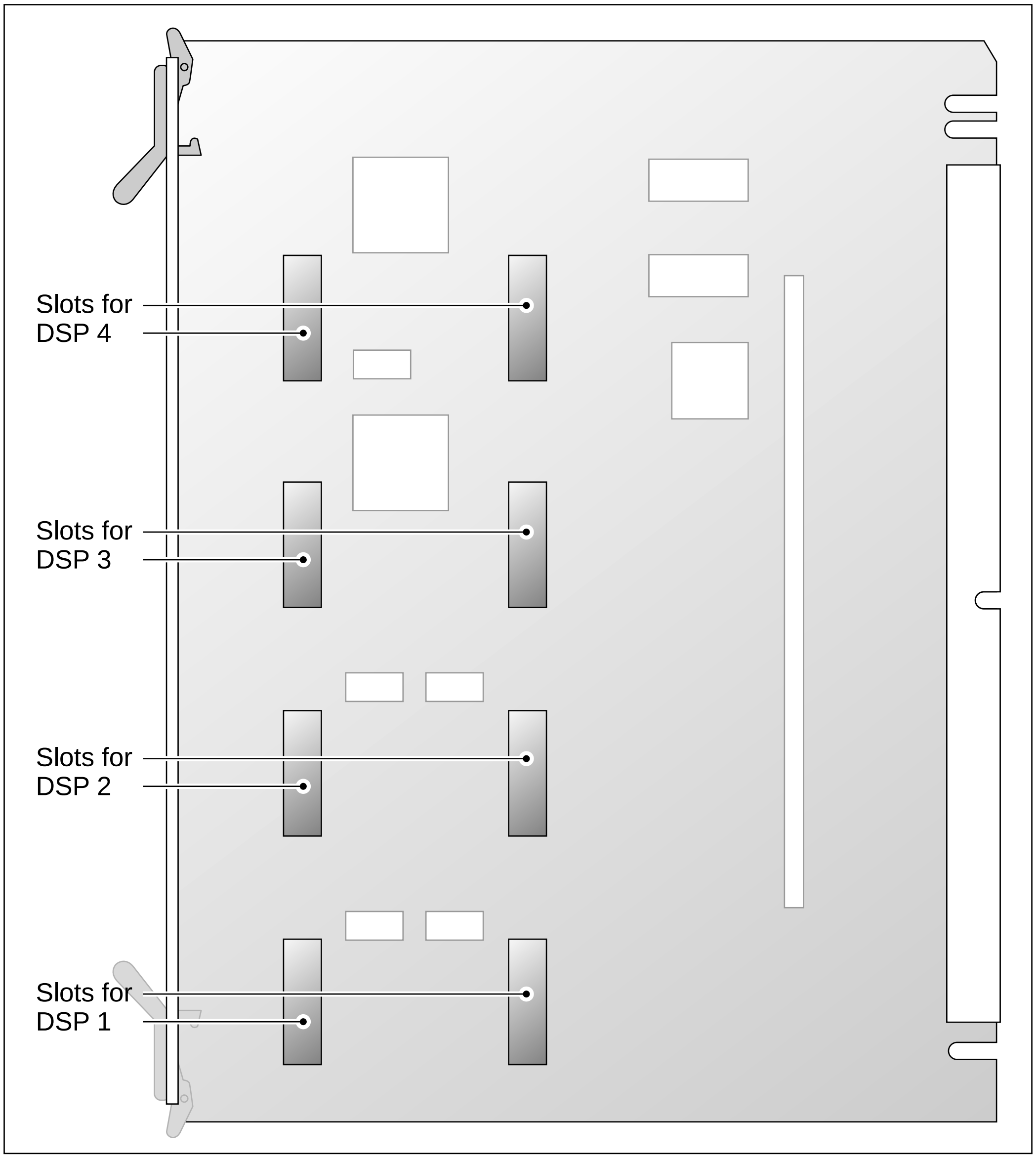
IPE versus Option 11

You can purchase double-wide MIG RLCs for IPE shelves and Option 11 cabinets. Because the dimensions of card slots in IPE shelves and Option 11 cabinets differ slightly, double-wide IPE cards are available in two varieties, each with its own order code, as outlined in the following table:

Destination	Order code
IPE shelf	NTDR70
Option 11 cabinet	NTDR71

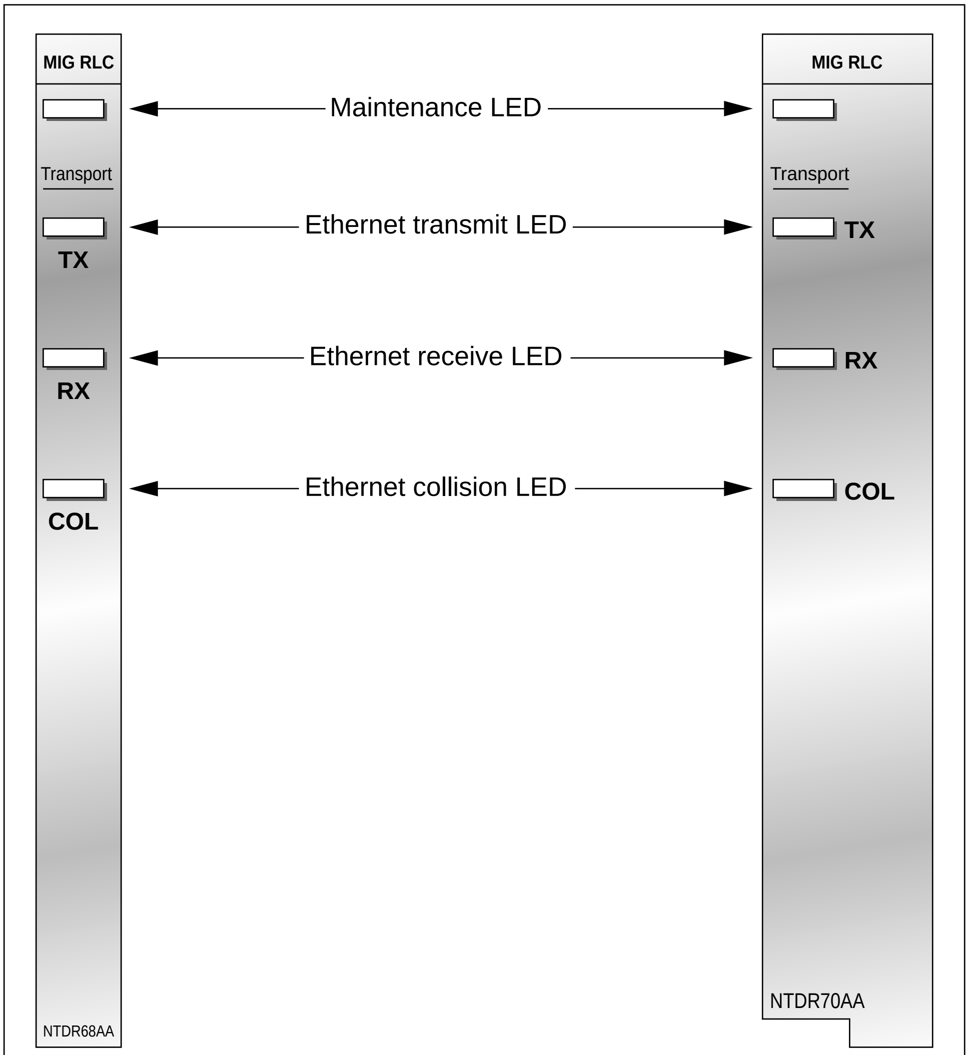
Regardless of order code, however, the motherboard of the 32-channel MIG RLC is the same circuit pack that is used for the 16-channel MIG RLC. This circuit pack is shown in the illustration on page 5. The MIG RLC motherboard conforms to the Common Features Specification for IPE line cards.

MIG RLC motherboard



G101387

MIG RLC faceplates: 16-channel and 32-channel



Note: The IPE version of the double-wide faceplate is pictured here. If the MIG RLC is installed in an Option 11 cabinet, the order code on the faceplate is NTDR71AA.

G101386

LED indicators

The red Maintenance LED on the faceplate indicates the basic health of the MIG RLC, just as with all other IPE line cards. Under normal conditions, the Maintenance LED lights under firmware control at power up, blinks three times after a successful self-test, and remains lit until the PBX enables the MIG RLC, at which time it goes out. If the PBX disables the MIG RLC, the Maintenance LED comes on and stays on.

- If, after the MIG RLC passes its self-test, the Maintenance LED comes back on, ensure that the card is enabled. (See PBX documentation for the correct procedure.) If the MIG RLC is enabled and the LED remains on, there is a problem at the PBX.
- If the LED blinks repeatedly at one-second intervals, reseat the card at the PBX by lifting the ejector tabs outward and pulling the MIG RLC toward yourself. This action breaks the connection between the line card and the backplane.

  After breaking this connection, reinsert the card completely into its slot. If the MIG RLC still does not complete a successful self-test, you must replace the line card.

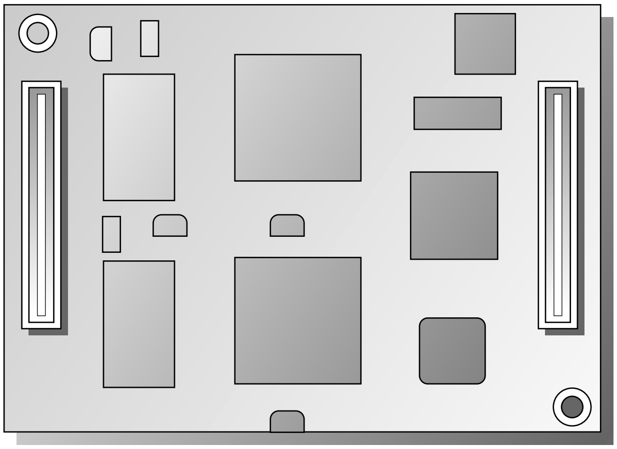
Three other faceplate LEDs monitor transmit and receive activity and collisions over the MIG RLC’s Ethernet interface. The 16- and 32-channel MIG RLC faceplates are shown on page 6 with the function of each LED labeled.

Note: The double-wide faceplate shown on page 6 is the IPE version. If the MIG RLC is installed in an Option 11 cabinet, the order code is NTDR71AA.

DSP application modules (NTDR73xx)

You can add up to four DSP application modules to the MIG RLC to extend your system’s voice processing capacity. Each module provides an additional eight channels of packet voice processing. The locations of DSP expansion slot pairings on the MIG RLC are shown on page 5. For help in determining the number of DSP application modules you need to increase your system’s call-processing capabilities to the desired level, refer to “Installing DSP application modules” on page 71, and the MIG RLC “System expansion worksheet” on page 338.

The illustration below shows a digital signal processor (DSP) application module, which holds two DSP devices. You can add up to four DSP application modules to your MIG RLC to increase the line card’s call processing capability by up to 32 channels. For the complete installation procedure, refer to “Installing DSP application modules” on page 71.



Remote Office DSP module (NTDR73xx)

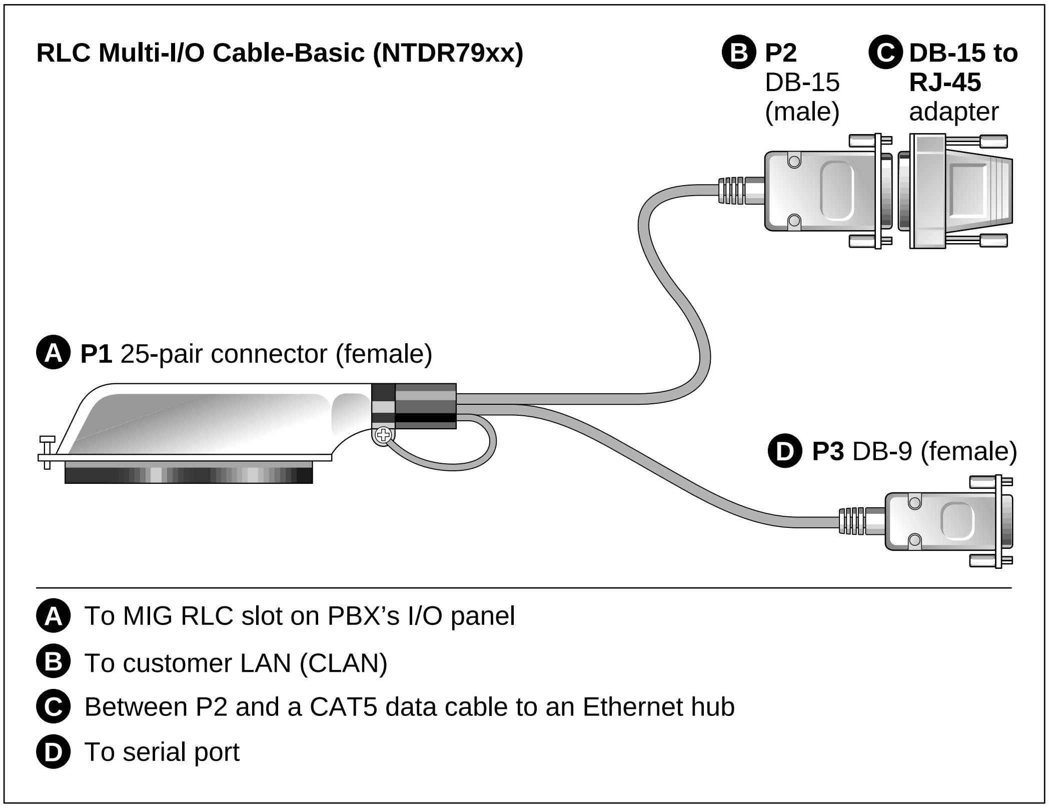
G101388

Meridian Internet Gateway Reach Line Card cables

MIG RLC cabling connections are made at the I/O panel of the shelf or cabinet in which the line card resides. Nortel Networks offers two cables that enable you to add the MIG RLC to a variety of existing network configurations.

RLC Multi-I/O cable–Basic (NTDR79xx) description

The following illustration shows the RLC Multi-I/O cable–Basic:



RLC Multi-I/O Cable-Basic (NTDR79xx)

B P2 DB-15 (male)
C DB-15 to RJ-45 adapter
A P1 25-pair connector (female)
D P3 DB-9 (female)
A To MIG RLC slot on PBX's I/O panel
B To customer LAN (CLAN)
C Between P2 and a CAT5 data cable to an Ethernet hub
D To serial port
G101389

This cable allows you to take advantage of the MIG RLC's basic capabilities. The package containing the MIG RLC includes one RLC Multi-I/O cable–Basic, which provides 10BaseT connectivity to the corporate Ethernet—for Voice over Internet Protocol (VoIP) access—and RS-232 connectivity to the serial port for administration and maintenance.

Note: The MIG RLC supports only 10BaseT Ethernet speeds.

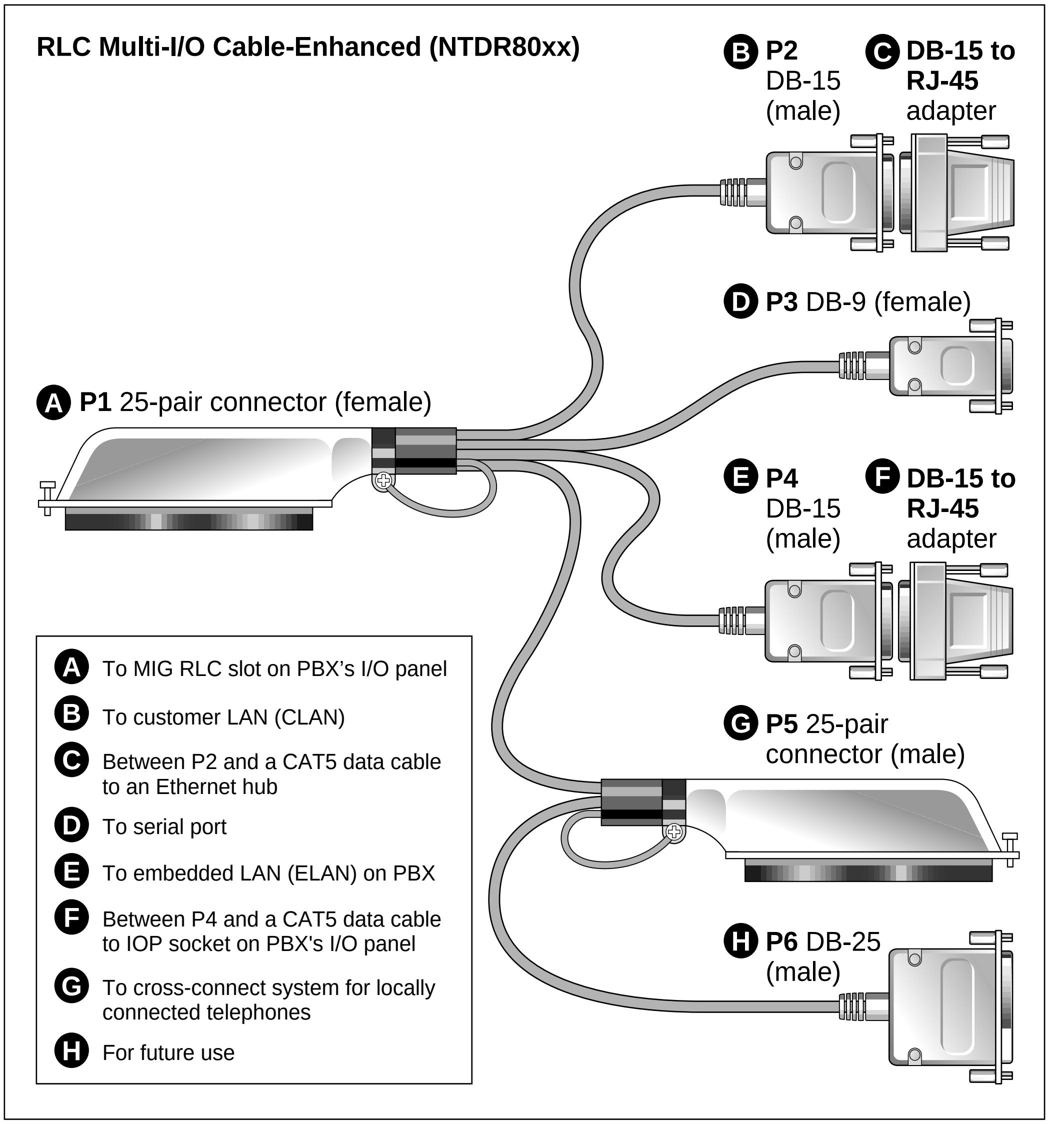
The following table describes the RLC Multi-I/O cable–Basic:

<table>
<tr><th>The connector labeled</th><th>is a</th><th>that transmits</th><th>and connects to the</th></tr>
<tr><td>P1</td><td>25-pair connector (female)</td><td>all signals</td><td>I/O panel.</td></tr>
<tr><td colspan="4"><b>Note:</b> If you are using a double-wide, 32-channel MIG RLC, insert P1 into the socket for the first of the two card slots occupied by the MIG RLC.</td></tr>
<tr><td>P2</td><td>DB-15 connector (male)</td><td>10BaseT signaling</td><td>CLAN Ethernet (customer LAN on the network).</td></tr>
<tr><td colspan="4"><b>Note:</b> P2 requires a DB-15 to RJ-45 converter (shipped with the cable).</td></tr>
<tr><td>P3</td><td>DB-9 connector (female)</td><td>RS-232 signaling</td><td>serial port connection for administration and maintenance.</td></tr>
</table>

The length of this cable, from the termination end of P1 to the termination end of any of the other plugs, is 0.6 m (2 ft).

RLC Multi-I/O cable–Enhanced (NTDR80xx)

The following illustration shows the RLC Multi-I/O cable–Enhanced.


RLC Multi-I/O Cable-Enhanced (NTDR80xx)
B P2 DB-15 (male)
C DB-15 to RJ-45 adapter
D P3 DB-9 (female)
A P1 25-pair connector (female)
E P4 DB-15 (male)
F DB-15 to RJ-45 adapter
G P5 25-pair connector (male)
H P6 DB-25 (male)
A To MIG RLC slot on PBX's I/O panel
B To customer LAN (CLAN)
C Between P2 and a CAT5 data cable to an Ethernet hub
D To serial port
E To embedded LAN (ELAN) on PBX
F Between P4 and a CAT5 data cable to IOP socket on PBX's I/O panel
G To cross-connect system for locally connected telephones
H For future use

G101390

Note: The MIG RLC supports only 10BaseT Ethernet speeds.

This cable enables you to use the MIG RLC's complete range of call processing capabilities. This cable adds connectivity to an existing V.35 Frame Relay network for call transport, and to the PBX's internal Ethernet for switch maintenance, to the connectivity supplied by the RLC Multi-I/O cable–Basic (see page 9). This cable also provides the flexibility to service locally connected telephones over MIG RLC channels not used for remoting purposes.

Note: V.35 functionality is not available in the initial release of the MIG RLC.

The following table describes the RLC Multi-I/O cable–Enhanced:

The connector labeled	**is a**	**that transmits**	**and connects to the**
P1	female 25-pair connector	all signals	I/O panel.
Note: If you are using a double-wide, 32-channel MIG RLC, insert P1 into the socket for the first of the two card slots occupied by the MIG RLC.			
P2	male DB-15 connector	10BaseT signaling	CLAN Ethernet (customer LAN on the network).
Note: P2 requires a DB-15 to RJ-45 converter (shipped with the cable).			
P3	female DB-9 connector	RS-232 signaling	serial port connection for administration and maintenance.
P4	male DB-15 connector	10BaseT signaling	ELAN Ethernet (PBX's embedded LAN).
Note: P4 requires a DB-15 to RJ-45 converter (shipped with the cable).			
P5	male 25-pair connector	TCM signaling	cross-connect to local telephones.
P6	male DB-25	V.35 signaling	Frame Relay Access Device (FRAD).
Note: P6 is reserved for future use.			

The length of this cable, from the termination end of P1 to the termination end of any of the other plugs, is 0.6 m (2 ft).

Operational characteristics

Introduction

The MIG RLC provides a number of unique features that distinguish it from other remoting products.

These features include

- configurable Quality of Service (QoS) transitioning technology
- variable security
- packet voice processing and dial-up trunking
- transparent operation
- Meridian telephone equipment compatibility

Configurable Quality of Service transitioning technology

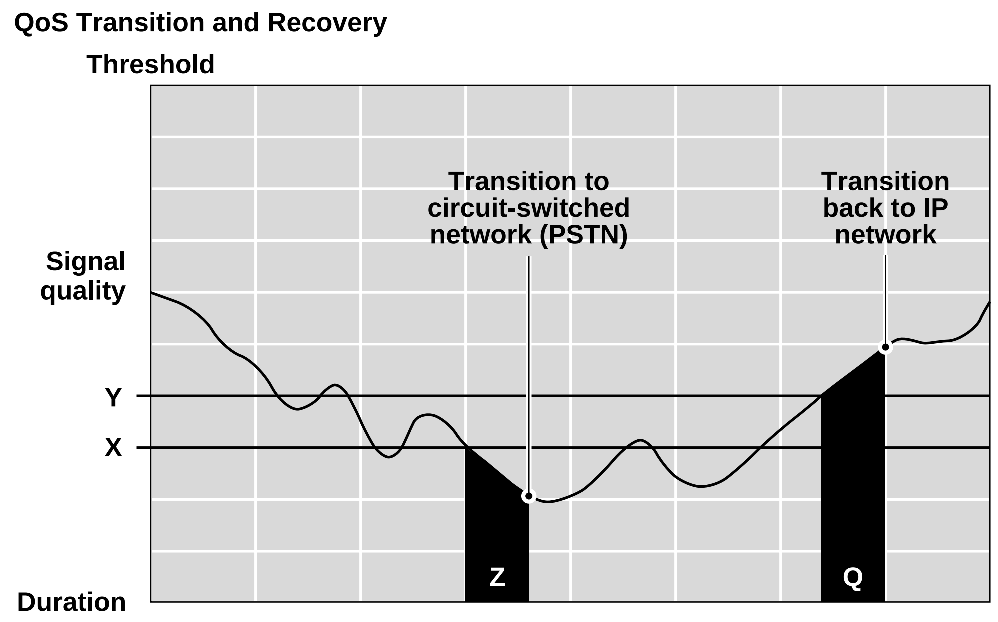
Communications between the MIG RLC in your office and the Remote Office 9150 unit at the remote site take place across the IP network using a 10BaseT Ethernet interface. You can configure the MIG RLC to switch automatically from the IP network to the circuit-switched network when the voice Quality of Service (QoS) falls below a predetermined threshold.

Both the MIG RLC and the Remote Office 9150 unit monitor the IP network's QoS constantly. If the QoS degrades, causing poor voice quality, the MIG RLC moves, or transitions, the call to the circuit-switched network. When the QoS returns to normal, the MIG RLC transitions the call back to the IP network.

The QoS transitions are accomplished using Nortel Networks' patented QoS transitioning technology. For detailed instructions on configuring the thresholds, refer to "Configuring Quality of Service" on page 183. For guidelines on evaluating and adjusting the QoS on your IP network, see Appendix A, "Network engineering guidelines."

How the Quality of Service transitioning technology works

The following illustration shows how the QoS transitioning technology works.



	Signal Degrade	Signal Recovery
Threshold (in terms of packet loss and decay)	X	Y
Duration in seconds	Z	Q

G101427

The following items describe the threshold and duration settings shown in the diagram. These settings are configured on the MIG RLC port for each remote unit.

Setting	Description
X	Represents the threshold where signal quality on the IP network has degraded enough to warrant call transitions to the circuit-switched network.

Setting	Description
Y	Represents the threshold representing acceptable signal quality on the IP network. When signal quality is good, calls continue to be processed on the IP network.
Z	Represents the amount of time that signal quality must be lower than the X threshold before calls are transitioned to the circuit-switched network.
Q	Represents the amount of time that signal quality must be higher than the Y threshold before calls are transitioned back to the IP network.

1. When the IP QoS falls below threshold X, the system waits for duration Z to determine if the QoS will return to normal.

2. If the QoS did not return to normal before duration Z passed, the MIG RLC establishes a PSTN network connection to the MIG RLC on the host PBX.

   The MIG RLC can make multiple PSTN connections (one every 30 seconds) depending on the bandwidth required to service all currently active calls.

   Voice quality can degrade while the dialup PSTN network connection is being established. Affected users are notified of the transition by a message sent to their telephone displays. Likewise, when service is restored to the IP network, users are notified by a message sent to their telephone displays.

3. Once the PSTN connection is established, calls are routed, 64 Kbps at a time, from the IP network connection to the PSTN connection. The system waits several seconds before moving the next 64 Kbps to determine if the IP connection has become more stable.

   As many calls as possible (to a maximum of 64 Kbps per B-channel) are moved from the IP connection to the PSTN trunk connection. High priority users are always moved first.

   Transitions are transparent to the users and can take place during a live call. The one exception is in the event of a complete network failure.

   Note: A slight degradation in voice quality can occur during the transition.

4. Both the MIG RLC and the Remote Office 9150 unit run an IP test to determine if the QoS on the IP network meets the standards you have configured. See “Offline IP network measurements” on page 17.
5. When the IP QoS exceeds the Y threshold, the system waits for duration Q to ensure that the QoS is stable enough to resume service on the IP network.
6. If the QoS continues to exceed the Y threshold, all active calls are moved back to the IP network and all new calls are placed over the IP network.

Quality of Service traffic measurements

As each voice packet is sent over the IP network, the MIG RLC monitors the following QoS parameters:

- average packet delay

  The delay is calculated using the following statistics gathered from the MIG RLC’s voice jitter attenuation buffer:

  - minimum packet holding time in the jitter buffer
  - maximum packet holding time in the jitter buffer
  - peak holding time in the jitter buffer
  - time-stamp values in the packet header

  By accumulating these statistics over time, the MIG RLC can calculate an average packet delay value through the IP network. As the system detects an increase in the average packet delay, it references the signal degrade threshold to determine when the transition to the PSTN connection should be made.

  See Chapter 7, “Administration,” for a detailed description of statistics.

- lost packets

  Lost packet statistics are calculated by accumulating the following packet header and voice decoder statistics:

  - voice decoder underrun
  - voice decoder overrun
  - out-of-sequence packet reception

Offline IP network measurements

Once the MIG RLC has reverted to using its PSTN connections, it must continually monitor the IP network to determine an appropriate time to restore voice traffic to the IP network as follows:

1. Pseudo voice traffic is placed on the IP network by both the MIG RLC and the Remote Office 9150 unit.

   This traffic is generated with a maximum bandwidth of no more than 16 Kbps and is sent in short bursts at a higher bit rate to approximate live voice traffic.

2. Both the MIG RLC and remote unit gather statistics based on the pseudo traffic to determine the congestion levels on the network. They use packet time stamps and sequence numbers to monitor the following parameters:

   - average end-to-end delay
   - average round-trip delay
   - average packet-to-packet jitter
   - average packet loss

3. When the parameters listed in step 2 fall within the predetermined threshold, the voice traffic is restored to the IP network.

   When restoring the connection back to the IP network, the system adds hysteresis to reduce the noise level during the transition. Hysteresis

   - prevents thrashing between the circuit-switched and IP networks
   - ensures that the voice QoS exists on the IP network for a predefined amount of time

Log reports and statistics

Configuration Manager provides a statistics log that identifies the number of QoS transitions (see “Caller Information Statistics screen” on page 223).

See Chapter 7, “Administration,” for a detailed description of log and statistic reports.

Transparent transition and recovery

Because both connection types transport packetized voice data, the transition from one to the other is completely transparent to the user and can take place during a live call. In most cases, the user notices only a considerable improvement in voice quality as the transition takes place.

The one exception is a complete IP network failure. In this situation, the user can experience a gap in service of several seconds (typically two to four seconds) while the dial-up PSTN connection is established. A message sent to the telephone display notifies the user of the transition. Likewise, when service recovers to the IP network, a similar message notifies the user.

Port-sharing options

Both dynamic port pooling and multi-user ports allow more efficient use of port resources because the activity of a single user, or a single telephone, does not dictate the usage of an entire port. Both options provide for more flexible, less restrictive use of the corporate telecommunications network.

Dynamic port pooling

Dynamic port pooling allows multiple users or stations to use individual ports on the host PBX in a time-share fashion. There is no correlation between the user or physical station and the TN or DN on the host PBX. When users sharing ports in a dynamic pool try to access a port, they receive the next available port in the pool regardless of the port’s TN or DN. If all ports in the pool are already active when a user attempts to make a call, that user hears a fast busy signal.

Multi-user ports

Like dynamic port pooling, multi-user ports also allow multiple users or stations to use individual ports on the host PBX in a time-share fashion. With a multi-user port, however, there *is* a specific correlation between the user or physical station and the TN or DN on the host PBX. When users sharing ports from a dynamic pool try to access a port, they receive access to the port if no one else configured to the port is already using it. Only one user can be active on a port at any given time.

Note: You can also configure a multi-user port to allow one user to access the same port from multiple locations, such as the corporate office and the home office.

Meridian Internet Gateway Reach Line Card security

Security configuration applies to all ports of a MIG RLC on a card-wide basis. You configure this information through the Configuration Manager. See “Remote connection configuration” on page 162.

The MIG RLC offers three levels of security, as described below.

Level	Description
no call security	The MIG RLC permits all incoming calls to access the host PBX regardless of source. **Note:** No call security is the default security level.
caller ID security	The MIG RLC compares the caller ID of the incoming call against the caller IDs entered for this remote unit through the Configuration Manager. If the caller ID does not match any of those entered in this unit’s Caller ID table, the MIG RLC denies PBX access to this call.
provisioned security	**1** If the call is from a remote unit to the MIG RLC, the MIG RLC compares the remote unit’s outbound security identifier with the inbound security identifier configured for the remote unit on the MIG RLC. If the call is from the MIG RLC to a remote unit, the remote unit compares the MIG RLC’s outbound security identifier with the inbound security identifier configured for the MIG RLC on the remote unit. **2** If the compared identifiers match, the receiving end accepts the call. If the compared identifiers do not match, the receiving end rejects the call.

Packet voice

All connections to the host PBX support the following features:

Voice compression

The MIG RLC supports G.711, G.726, and G.729A voice compression standards. You can assign different voice compression algorithms to individual ports. This feature allows you to configure different voice QoS for different users.

Voice jitter attenuation buffer

The MIG RLC's dynamic voice jitter attenuation buffer compensates for the uneven manner in which voice packets are received over a given period of time across data networks. This buffer allows packets that might arrive unevenly to be collected and relayed evenly over an equivalent period of time.

Packet loss handling techniques

The MIG RLC uses packet loss handling techniques to accommodate missing packets or packets received too late to be processed into the real-time voice stream.

Silence suppression algorithm

To save bandwidth, a silence suppression algorithm prevents packet transmission during periods when voice activity detection determines that there is no voice data present. The receiving end inserts comfort noise to assure the user that the line is still active.

Echo cancellation

The MIG RLC performs echo cancellation in accordance with ITU G.168, and cancels echo with a tail length of up to 32 milliseconds (32 ms).

Dial-up trunking

The MIG RLC supports Meridian digital trunks for remote connections. When using circuit-switched connections to the Remote Office 9150 unit, the MIG RLC shares the Meridian 1 digital trunks (ISDN PRI) to communicate with the remote location.

QoS transitioning technology

When used in Voice over IP (VoIP) mode, the MIG RLC supports ISDN PRI interfaces for local calling. It also supports QoS transitioning technology. Through this technology, you can configure the MIG RLC to switch voice traffic from the IP interface to ISDN BRI lines on the circuit-switched network if the IP network's QoS falls below a threshold that you choose. You can select an acceptable transition threshold from among ten defined settings. You can configure the MIG RLC to initiate the transition call from the host site or the remote site to achieve maximum savings on connection costs.

For a detailed explanation of how the QoS transition technology works, see "Configurable Quality of Service transitioning technology" on page 13. For exact configuration procedures, see "Quality of Service transitioning technology" on page 163.

Bandwidth utilization

The voice compression algorithm that you choose when configuring DSP resources determines the bandwidth utilization of the MIG RLC. The MIG RLC currently supports the following compression algorithms:

Supported algorithms	Compressed bit rate
G.711	64 Kbps
G.726	32 Kbps
G.729A	8 Kbps

Dynamic trunk bandwidth allocation

The MIG RLC dynamically allocates available trunk bandwidth in circuit-switched mode to maximize its use. That is, as calls are initiated and bandwidth requirements increase, additional trunk connections are established.

Call-On-Demand

The MIG RLC supports full Call-On-Demand (COD) functionality, including a configurable minimum call duration timer and an idle timer. COD refers to the way host trunk connections are handled. In the COD mode of operation, a host connection is not established until the user places a call to a host DN. The COD connection stays active until the minimum call duration timer expires, at which time the host connection is terminated, if idle. If another call is initiated toward the host before the timer expires, the timer is reset and tracks the last call established. There is a single timer per site.

DN priority

The MIG RLC provides multiple priority levels:

- high
- normal
- circuit-switched only
- IP only

If this feature is used, you must configure an amount of bandwidth to save for privileged DNs and identify the privileged DNs via the Configuration Manager. The MIG RLC uses the extra bandwidth for high priority DNs. When only enough bandwidth for the high priority DNs is available and a normal priority DN tries to dial out, the telephone gets a fast busy signal. For details on configuring DN priority, see “RLC port configuration” on page 162.

Online/offline table

The MIG RLC uses a user-configurable table to establish or terminate host connections at specified times of the day. This feature avoids excessive connection charges for the host connection when it is not in use. For details on configuring the online/offline table, see “To configure the online/offline table” on page 192.

Transparent operation

The MIG RLC provides full Meridian 1 PBX functionality to as many as 32 users at a remote location as though their telephones were in the same location as the host PBX.

Telephone hardware compatibility

By emulating MIG RLC-compatible models of the Meridian digital telephone and providing access to the corporate data network, the MIG RLC allows people at remote locations to function as if they were located within the corporate office. Meridian digital telephone equipment that is compatible with the MIG RLC includes the following telephone models and modules:

Models		Modules
M2008D	M3310	Add-on modules
M2008HFD	M3820	Key-expansion modules
M2616D	M3902	
M2616CT	M3903	
M2216D	M3904	
M3110	M3905	

Note: The M2006 and M3901 telephones are also supported, but can be used only for local-controlled calls. These telephones do not have displays, which are required for host PBX functionality.

Data channel adapters

The Remote Office uses the following types of data channel adapters:

- Analog Telephone Adapters (ATAs)
- Meridian Communication Adapters (MCAs)

All MCAs use the secondary data channel of the TCM telephone interface and require an entire clear channel of a BRI connection. See “Understanding port relationships” on page 104 for information about port assignment for data channel adapters.

A single-wide MIG RLC handles up to four data channel adapters. A double-wide MIG RLC handles up to seven data channel adapters.

Nortel Networks CTI and ACD applications

The MIG RLC operates properly with all Nortel Networks computer telephony interface (CTI) and automatic call distribution (ACD) applications.

PBX hardware and software compatibility

Hardware

The MIG RLC is compatible with the following Meridian 1 systems:

- any system capable of supporting the XDLC circuit pack
- Meridian 1 Options 11(C), 11(C)-mini, 11(E), 21(E), 51(C), 61(C), 71(C), and 81(C)

  Note: Older Meridian 1 systems that have been upgraded with IPE modules can also utilize MIG RLCs.

Software

The MIG RLC is compatible with Meridian 1 software Release 17 and above.

Note: You can use the MIG RLC with Release 15 and above, but the data port configuration is slightly different. See the table on page 106 for further details.

How the Reach Line Card works

Introduction

A network based on the MIG RLC processes calls in one of two modes:

- host-controlled mode
- local-controlled mode

This section covers procedures for making calls using both of these call-processing modes.

Outgoing call process

You can initiate an outgoing call by either picking up your telephone's handset or pressing a line appearance key. There are two types of appearance keys:

- host call appearance keys, used to make calls to the host site
- local call appearance keys, used to make calls to another station at the branch office, or to make and receive calls through the local PSTN

Details of the outgoing call process appear in the illustrations and procedures on pages 27–31.

Incoming call process

When a call is placed through the host PBX to a user at a remote location, a connection is made from the MIG RLC to the remote unit. The host PBX completes the call normally. If a connection cannot be established, the call rings until the host PBX forwards it to voice mail.

Host-controlled calls

When you make a call to someone at your host site, or when someone at your host site calls you, the call is processed in the host-controlled mode. Such calls are routed through the host PBX. Details of host-controlled call processing appear in the illustrations and procedures on pages 27–30.

Local-controlled calls

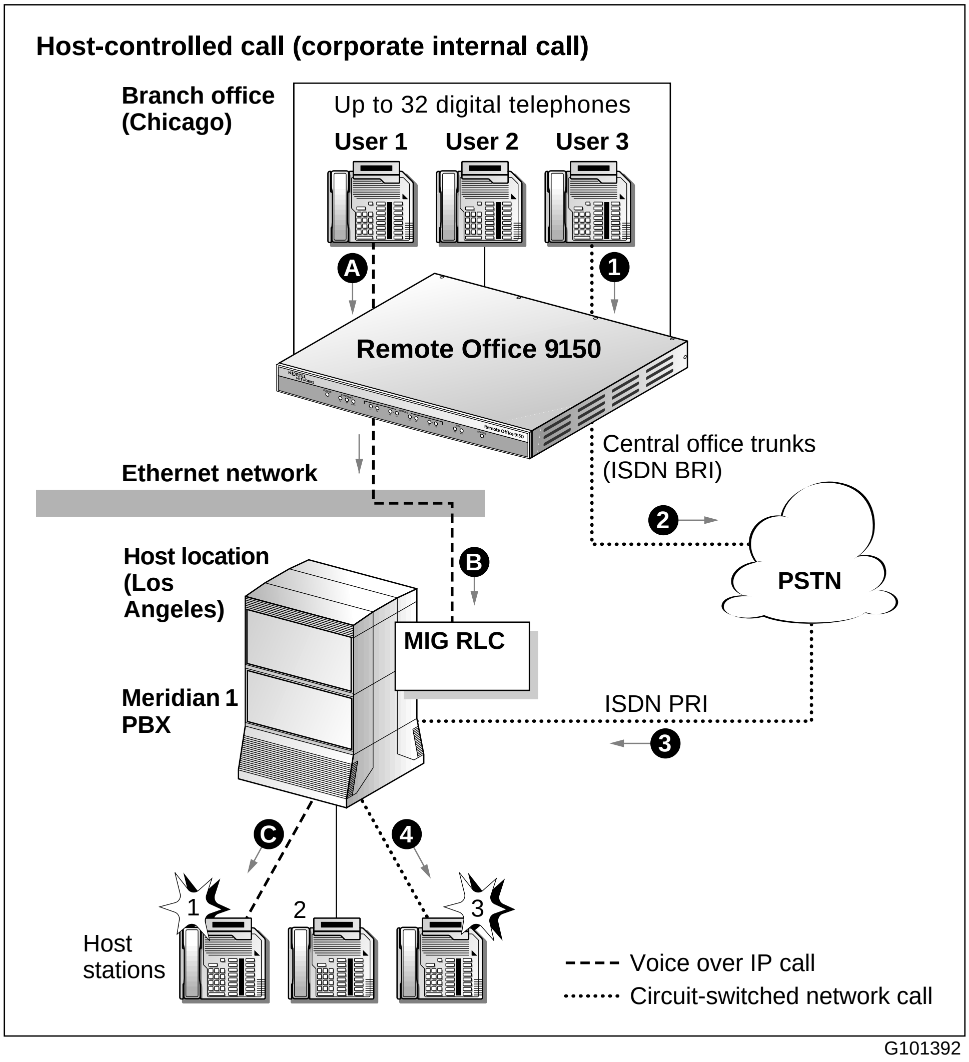
When a user presses one of the local call appearance keys and dials the DN of another local call appearance key, the Remote Office 9150 unit processes the call. When the user initiates a call by pressing one of the local call appearance keys and then dials a local trunk access code, the local PSTN processes the call. Both of these types of calls are processed in the local-controlled mode. The host PBX is not involved in local-controlled calls. Details of local-controlled call processing appear in the illustrations and procedures on pages 31 and 32.

Quality of Service transitioning technology

When using Voice over IP, if the QoS over the IP network falls below a predefined threshold, you can configure the system to automatically route voice traffic away from the IP network connection to the circuit-switched network connection. See “Configurable Quality of Service transitioning technology” on page 13 for a description of this feature.

Call scenario 1: Host-controlled—internal corporate call

The following diagram shows how a call is routed when making a host-controlled call to the corporate office.


Host-controlled call (corporate internal call)
Branch office (Chicago)
Up to 32 digital telephones
User 1
User 2
User 3
A
1
Remote Office 9150
Ethernet network
Central office trunks (ISDN BRI)
2
PSTN
Host location (Los Angeles)
B
MIG RLC
Meridian 1 PBX
ISDN PRI
3
C
4
1
2
3
Host stations
Voice over IP call
Circuit-switched network call
G101392

The network that is used to route the host-controlled call is transparent to the user, and the dialing requirement is the same for both. Calls work the same way in reverse, from host PBX site to the Remote Office 9150 site.

Voice over IP network call

1 User 1 presses the host call appearance key.

Result: User 1 hears a dial tone. This indicates that the connection to the MIG RLC over the IP network was successful.

2 User 1 dials a telephone number (such as the extension number of host station 1).

Result: The dialed digits are sent by the Remote Office 9150 unit as packets across the Ethernet network. The MIG RLC converts the packets to the format required by the PBX. The PBX then converts the data to voice and routes the call to host station 1.

Circuit-switched network call

1 User 3 presses the host call appearance key.

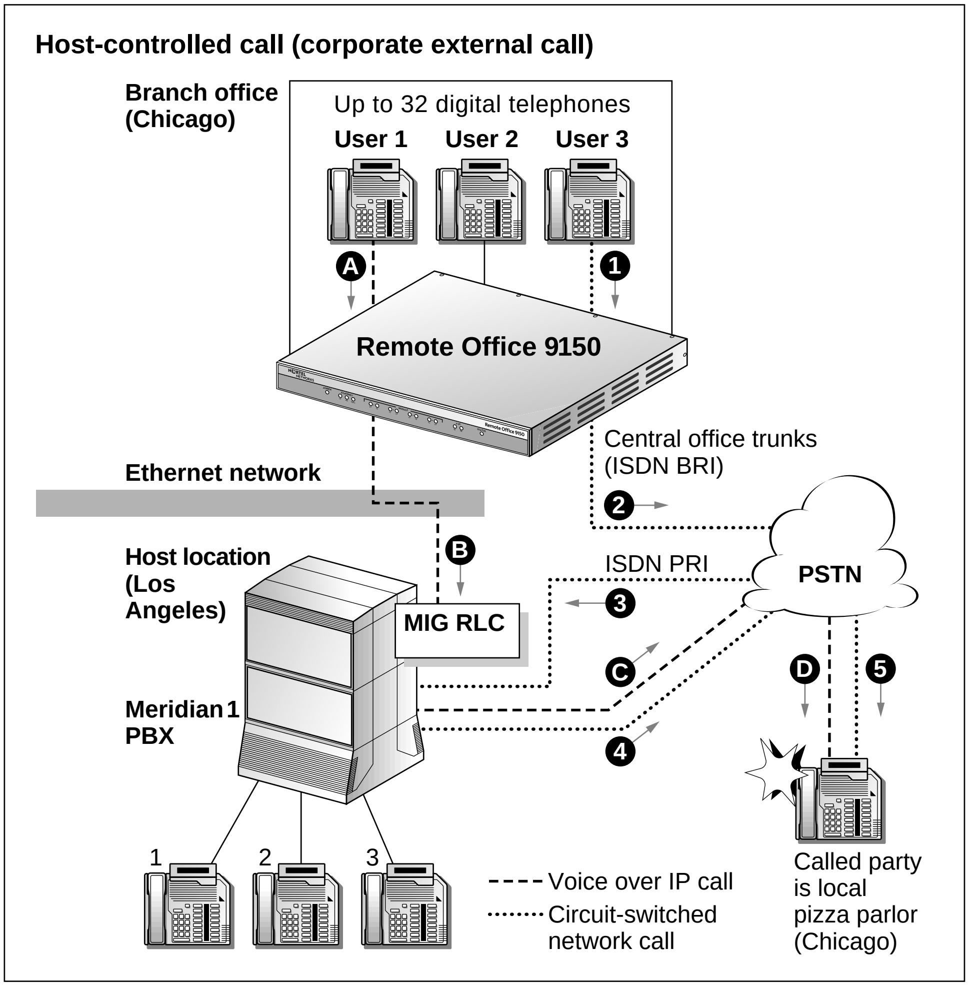
Result: User 3 hears a dial tone. This indicates that the connection to the MIG RLC over the circuit-switched network was successful.

2 User 3 dials the telephone number (such as the extension number of host station 3).

Result: Dialed digits are sent across the PSTN through the PBX to host station 3.

Call scenario 2: Host-controlled—external corporate call

The following diagram shows how a call is routed when making a host-controlled call to a party outside the organization.


Host-controlled call (corporate external call)
Branch office (Chicago)
Up to 32 digital telephones
User 1
User 2
User 3
A
1
Remote Office 9150
Ethernet network
Central office trunks (ISDN BRI)
2
PSTN
ISDN PRI
3
B
Host location (Los Angeles)
MIG RLC
C
D
5
Meridian 1 PBX
4
1
2
3
Voice over IP call
Circuit-switched network call
Called party is local pizza parlor (Chicago)

G101393

The network used to route the call is transparent to the user, and the dialing requirement is the same for both. Calls work the same way in reverse, through the host PBX site to the Remote Office 9150 site.

Voice over IP network call

1 User 1 presses the host call appearance key.

Result: User 1 hears a dial tone. This indicates that the connection to the MIG RLC over the IP network was successful.

2 User 1 dials the external telephone number.

Result: The dialed digits are sent by the Remote Office 9150 unit as packets across the Ethernet network. The MIG RLC converts the packets to the format required by the PBX. The PBX then converts the data to voice and routes the call through the PSTN to the called party.

Circuit-switched network call

1 User 3 presses the host call appearance key.

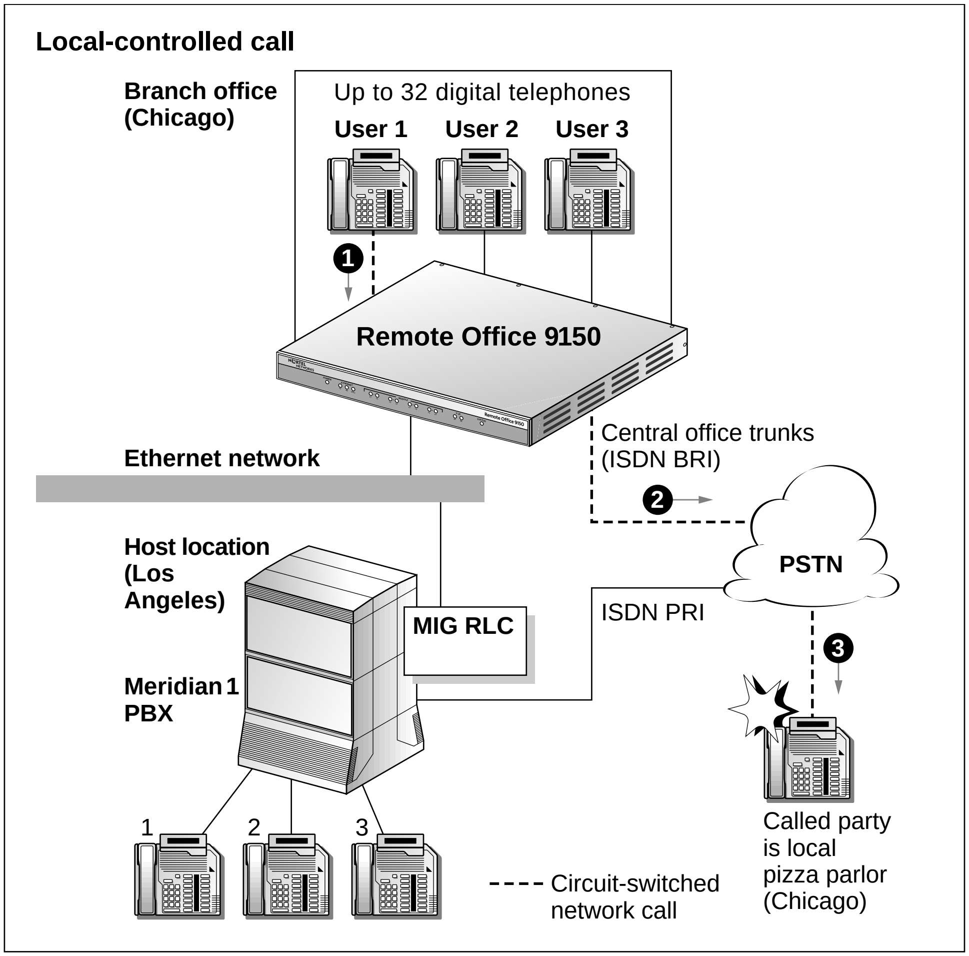
Result: User 3 hears a dial tone. This indicates that the connection to the MIG RLC over the circuit-switched network was successful.

2 User 3 dials the external telephone number.

Result: Dialed digits are sent across ISDN BRI through the PSTN, through the host PBX to the called party.

Call scenario 3: Local-controlled mode—local call

The following diagram shows how a call is routed when making a call within the Remote Office 9150 unit’s local area.


Local-controlled call
Branch office (Chicago)
Up to 32 digital telephones
User 1
User 2
User 3
1
Remote Office 9150
Ethernet network
Central office trunks (ISDN BRI)
2
PSTN
Host location (Los Angeles)
MIG RLC
ISDN PRI
3
Meridian 1 PBX
1
2
3
Circuit-switched network call
Called party is local pizza parlor (Chicago)

G101394

Local call

1 User 1 presses the local call appearance key and hears a dial tone from the Remote Office 9150 unit.

2 User 1 then dials a trunk access code (such as #8) and hears a dial tone from the Central Office (PSTN).

Note: If all trunks are busy and unavailable, then User 1 hears a fast busy signal.

3 User 1 dials the telephone number (the pizza parlor in this example). The dialed digits are sent across the ISDN BRI connection through the PSTN to the called party.

Environmental requirements

Introduction

This section includes information concerning the range of environmental conditions under which the MIG RLC functions properly.

Environmental conditions

The MIG RLC withstands the following environmental conditions without any performance degradation or damage.

Note: In this section, the phrase *short term* equates to 72 consecutive hours with a maximum of 15 days per year. The temperature ratings are for the environment of the circuit and not the total system.

Specification	Condition
Operating temperature	
Normal	+10 to 45°C
Short Term	0 to +55°C
Operating humidity	
Normal	10% to 95% (noncondensing)
Short Term	5% to 95% (noncondensing)
Storage	
Temperature	-50 to +70°C
Humidity	5% to 95% RH (noncondensing)

Chapter 2

Planning for installation

In this chapter

Overview

Introduction

To get the most out of your company’s investment in the Meridian Internet Gateway Reach Line Card (MIG RLC), you must plan and prepare.

Preinstallation preparation

Preinstallation preparation consists of

- planning for the remoting needs of the company
- preparing the site
- unpacking and inspecting the equipment
- taking inventory

System resources management

The MIG RLC offers you a number of methods to manage system resources. These methods include

- QoS transitioning technology
- host connection management
    - variable trunk connection accessibility (permanent or on-demand trunks)
    - call timers (on-demand trunks only)
- variable security
- online/offline scheduling

Network considerations

When you implement a MIG RLC-based system, consider ways that this system can affect your current telecommunications and data networks.

Administration PC

The administration software is Windows-based and is installed on a PC. For details on ways that you can connect an administration PC to the MIG RLC and the hardware and software requirements for using the administration software, see page 55.

Planning for future growth

The MIG RLC can change as your telecommunications needs change. See page 59 for suggestions on planning for system expansion.

Preinstallation preparation

Introduction

Preinstallation preparation consists of

- preparing the site
- planning for the remoting needs of the company
- planning the installation of the equipment
- planning the deployment of new capabilities
- unpacking and inspecting the equipment
- taking inventory

Preparing the site

Site preparation involves considering environmental, structural, and electrical factors. System planners and installers must consider site-specific limitations, as well as company-specific guidelines in this process. More information on site-preparation from an equipment standpoint is available in the following documents:

- *Meridian 1 Installation and Planning* (NTP 553-3001-120)
- *Meridian 1 System Engineering* (NTP 553-3001-151)
- *Meridian 1 Power Engineering* (NTP 553-3001-152)
- *Meridian SL-100 Intelligent Peripheral Equipment-IPE* (NTP 555-4001-129)

Planning for your remoting needs

Begin your remoting plan by determining the total number of simultaneously remote telephone calls you want to support on your network. This tells you the total number of MIG RLC channels that you need.

MIG RLC requirements

Once you have determined the total number of MIG RLC channels that you need in your network, you can determine the total number of MIG RLCs that you need at your host site. Remember that you must configure all channels from a single Remote Office 9150 unit to the same MIG RLC. You cannot provide service to one Remote Office 9150 unit from more than one MIG RLC.

For every group of 16 simultaneous calls that you want your system to support, you must commit one card slot in your PBX and one 16-channel MIG RLC. If you have more than 16 channels in your remote network, you need at least one 32-channel MIG RLC. Refer to the table below for calculating exact MIG RLC requirements in your remote network.

Note: Include planning for future expansion when determining the total number of MIG RLC channels that you need in your network.

The following table gives some guidelines for choosing the proper MIG RLC for your remoting needs:

IF the number of simultaneous calls is	THEN you need
less than 17	a 16-channel MIG RLC.
between 17 and 32	a 32-channel MIG RLC.
greater than 32	to consult with your Nortel Networks distributor.

DSP requirements

In addition to determining the number of MIG RLCs you need for your remote network, the total number of simultaneous remote telephone calls that you want to support also determines the number of DSP application modules that you need.

- Each remoted telephone call requires one DSP channel.
- One DSP application module holds eight channels, providing eight additional voice paths between host and remote sites.

Both the 16-channel and 32-channel versions of the MIG RLC come equipped with the equivalent of one built-in DSP application module. Thus, the basic 16-channel and 32-channel line cards each provide non-blocking service for up to 8 users.

Examples

The following sample configurations illustrate the capacities of a few common MIG RLC and DSP combinations:

- The basic 16-channel MIG RLC supports 16 users with 2:1 blocking (eight simultaneous calls provided by eight on-board DSP channels).
- When you add one DSP application module to the 16-channel MIG RLC, this supports as many as 16 users in a non-blocking configuration (16 DSP channels providing call processing for 16 simultaneous calls).
- The basic 32-channel MIG RLC supports 32 users with 4:1 blocking (eight simultaneous calls provided by eight on-board DSP channels).
- When you add three DSP application modules to the 32-channel MIG RLC, they support as many as 32 users in a non-blocking configuration (32 DSP channels providing call processing for 32 simultaneous calls).

Installation planning

Make an outline of cable routing between the I/O panel of the shelf that will house the MIG RLC and the following components:

- your switch’s Ethernet port (external Ethernet)
- your switch’s serial port
- the I/O-panel connection to the IOP (input-output port) card for access to the switch’s internal Ethernet, or ELAN
- your Frame Relay Access Device (FRAD)—unavailable in the initial release
- the cross-connect device to the local telephones you want to serve with the MIG RLC channels not used for remoting purposes

Note: The last three connections are not required for correct MIG RLC operation. These connections are only available if you are using the RLC Multi-I/O cable–Enhanced. See page 11 for more information on this cable.

Deployment planning

Include the MIG RLC configuration settings for each station at each remote site and for each port at the host site in your deployment plan. Use Appendix B, “Planning forms,” on page 317 to help you with this task.

Before configuration can take place via the Configuration Manager, you must configure PBX voice and data ports for each MIG RLC channel. See “Configuring remote and network ports” on page 106.

Checklists

The Installation checklist on page 42 provides a checklist for those responsible for the installation to ensure complete installation and configuration.

Planning forms

Appendix B, “Planning forms,” contains the following forms on which you can record and store your configuration plans:

- MIG RLC
  - Connection Information—16 ports
  - Connection Information—32 ports
  - Online/Offline Table Configuration
  - System expansion worksheet
- Remote Office 9150
  - Configuration Information—Stations
  - Configuration Information—ISDN BRI Modules
  - Configuration Information—Network Connections
  - Configuration Information—Dialing Plans
  - System expansion worksheet

You can also find these forms on the Nortel Networks web site at http://www.nortelnetworks.com/remoteoffice.

Unpacking and inspecting the equipment

Unpack the equipment and inspect it for damage. Follow these general precautions, which are recommended by computer and telephone equipment manufacturers:

- Remove items that generate static charge from the installation site.
- Use antistatic spray if the site is carpeted.
- Ground yourself before handling any equipment.
- Remove the equipment carefully from its packaging.
- Visually inspect the equipment for obvious faults or damage.

  Immediately report any damaged component to your Nortel Networks customer support representative and the carrier who delivered the equipment.
- Hold any non-enclosed circuit cards by their nonconducting edges, and keep them in their antistatic bags until you are ready to install them.
- Do not stack the non-enclosed circuit cards on top of each other.

Taking inventory

After you unpack and visually inspect the equipment, and before you begin installation, verify that all the equipment is at the site. Check the equipment you received against the shipping documents. Report any shortages to your Nortel Networks customer support representative immediately.

Installation checklist

When you or your telecom manager are preparing to perform the installation, use the following checklist to provide a means of ensuring that all the required installation steps and processes are completed properly and completely.

Meridian Internet Gateway Reach Line Card

Installation checklist

Page 1 of 6

Use this checklist to ensure that all installation tasks are completed.

Check	Task	For details, see
Planning		
❒	Review the Release Notes for last-minute product updates.	*Remote Office and MIG RLC Release Notes* (NTP 555-8421-102).
❒	Ensure you have the latest firmware and software.	*Remote Office and MIG RLC Release Notes* (NTP 555-8421-102).
❒	Ensure that your PBX platform and software release support the MIG RLC.	“PBX hardware and software compatibility” on page 24.
❒	Ensure that your PBX supports XDLCs.	documentation for your PBX.
❒	Ensure that a slot is available on the PBX IPE shelf for each MIG RLC. Order additional shelves if necessary. **Note:** NT8D37AA IPE cabinets utilize split-slot wiring. If you have one of these cabinets, your MIG RLCs can only reside in slots 0, 4, 8, and 12 without rewiring the slot. To use any other slot, you will need to rewire part of the IPE backplane using cable NT8D81AA (A0359946).	your Nortel Networks distributor.
❒	You can route calls over the IP network, the circuit-switched network, or both. Determine, at a high level, what you must do to implement these call routing methods.	“Deployment options” on page 60.

Meridian Internet Gateway Reach Line Card

Installation checklist

Page 2 of 6

Check	Task	For details, see
❒	If you want to use the IP network to route calls, evaluate the IP network to determine if the network infrastructure can support voice traffic.	■ your data network administrator ■ Appendix A, “Network engineering guidelines”
❒	Plan the installation and cabling of MIG RLCs.	Chapter 2, “Planning for installation.”
❒	Decide on the administration PC setup.	“Administration PC” on page 37.
❒	Obtain the cables that you need to establish the network connections.	“Meridian Internet Gateway Reach Line Card cables” on page 9.
❒	Gather the configuration information (network addresses, connection numbers, online/offline schedule, QoS thresholds, and so on).	■ “Deployment options” on page 60 ■ Appendix B, “Planning forms”
❒	Plan MIG RLC port assignments.	“Connection Information—16 ports” on page 324 or “Connection Information—32 ports” on page 329 depending on your MIG RLC.
PBX configuration		
❒ ❒	Configure the PBX to recognize each MIG RLC as an XDLC. Verify that the PBX recognizes each MIG RLC as an XDLC.	documentation for your PBX.
❒	If you want to use the circuit-switched network to route calls, ensure that ISDN PRI trunks are installed and configured on the PBX for both voice and data.	configuration on your PBX.

Meridian Internet Gateway Reach Line Card

Installation checklist

Page 3 of 6

Check	Task	For details, see
❒	Ensure that there is sufficient capacity on the trunks for the extra traffic involved in remoting operations.	configuration on your PBX.
❒ ❒	Configure a voice or data port on the PBX for each remote user. (These ports are associated with Remote ports on the MIG RLC.) Configure a data port on the PBX for each remote unit connection. (These ports are associated with Network ports on the MIG RLC.)	documentation for your PBX.
Hardware and software installation		
❒	Install DSP application modules on the MIG RLC, if required.	“Installing DSP application modules” on page 68.
❒	Install and cable each MIG RLC.	■ “To install a MIG RLC” on page 76 ■ “To cable a MIG RLC” on page 77
❒	Install the software from the product CD-ROM or the Nortel Networks web site.	“Installing the software” on page 67.
MIG RLC configuration		
❒	Configure the IP address, subnet mask, and default gateway on the MIG RLC.	“Using the Configuration Wizard to perform initial configuration” on page 67.

Meridian Internet Gateway Reach Line Card

Installation checklist

Page 4 of 6

Check	Task	For details, see
❒	If you want to use the PBX's administration terminal to administer the MIG RLC, configure the IP address and subnet mask of the MIG RLC's ELAN port.	"Configuring the Reach Line Card's IP interface" on page 159.
❒	Configure the following items, as required, to create the communication paths between the MIG RLC and the remote unit: ■ IP network: remote unit's IP address ■ circuit-switched network: remote unit's telephone number ■ security level and, if required, security identifier	■ "Using the Configuration Wizard to perform initial configuration" on page 67 ■ "To configure remote connection settings" on page 178
❒	Configure a Remote port on the MIG RLC for each user. **Note:** A Network port for each remote unit is created when you create the circuit-switched communication path with the Configuration Wizard.	Chapter 6, "Configuring the Meridian Internet Gateway Reach Line Card."
❒	Configure an online/offline schedule for each remote unit, if required.	Section C: "Online/offline table," on page 187. **Note:** A blank online/offline schedule can be found in the Online/ Offline Table section of Configuration Manger.

Meridian Internet Gateway Reach Line Card

Installation checklist

Page 5 of 6

Check	Task	For details, see
Remote unit configuration		
❒	Ensure that the remote unit is configured with the information it needs to establish connections with the MIG RLC.	the *Installation and Administration Guide* for the remote unit.
❒	Ensure that a station is configured for each user on the Remote Office 9150 unit.	*Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215)
Network configuration		
❒	Configure network devices ■ so that voice traffic is not constrained or congested ■ to maximize network efficiency for Voice over IP service	■ your data network administrator. ■ Appendix A, “Network engineering guidelines”
 ❒ ❒	Ensure that voice calls can be sent or received over the following: ■ IP network ■ circuit-switched network	your data network administrator.
❒ ❒	Ensure that processing of voice and data traffic over the IP network performs as expected. Adjust QoS settings, if required.	■ your data network administrator ■ your telecom network administrator ■ Appendix A, “Network engineering guidelines”
Testing		
❒	Ping the MIG RLC and ensure that it is recognized as a device on the network.	“Testing the connections” on page 94.

Meridian Internet Gateway Reach Line Card

Installation checklist

Page 6 of 6

Check	Task	For details, see
❐	Ensure that calls can be made and received on each MIG RLC port.	“Testing the connections” on page 94.
Administration		
❐	Plan for administration training and technical support.	■ Chapter 7, “Administration” ■ Chapter 8, “Troubleshooting”

System resources management

Introduction

The MIG RLC offers you a number of methods to manage system resources. These methods include

- QoS transitioning technology
- host connection management
  - variable trunk connection accessibility (permanent or on-demand)
  - call timers participate in management of on-demand trunks
- online/offline scheduling
- variable security

Quality of Service transitioning technology

On IP networks, traffic congestion can result in poor voice quality or lost connections. You can configure the MIG RLC to move call processing from the IP network to the circuit-switched network. When QoS on the IP network returns to acceptable levels, call processing is moved back to the IP network. The QoS thresholds (level and duration) defined on the MIG RLC determine the point at which the transition occurs.

Host connection management

Connections to the host PBX can be managed in three ways:

- putting the remote site in offline mode so that it cannot receive or make calls through the host PBX
- defining a trunk connection as permanent or on-demand
- defining call duration and idle timers, if the trunk connection is defined as on-demand

Call-on-demand

The MIG RLC supports full call-on-demand (COD) capability. In COD mode, the MIG RLC does not establish a connection to the host site until the user places a call to a host DN.

A configurable minimum call duration timer and an idle timer track the duration of trunk connections. The COD connection stays active until this timer expires, at which time the host connection is terminated. If the MIG RLC initiates another trunk connection to the host before the timer expires, the timer is reset and tracks the last call established. There is a single timer per site.

Online/offline schedule

You can configure an online/offline schedule on the MIG RLC to control when remote sites can make and receive calls through the host PBX, when operating in circuit-switched mode.

Configure offline entries for the following situations:

- times when remote users should not make or receive calls, such as during evenings and weekends
- to prevent remote sites from staying online permanently, thereby eliminating unwanted telephone access charges

When the MIG RLC processes an offline entry, it instructs the remote site to go offline for a specified number of hours and minutes. The number of hours and minutes the remote site stays offline is the difference between the offline entry being processed and the next online entry.

For example, an offline entry is configured at 6:00 p.m. The next online entry is configured at 9:00 a.m. the next day. When the MIG RLC processes the 6:00 p.m. entry, it instructs the remote site to go offline for 15 hours.

When going offline, a timer is activated at the remote site. When the timer expires (in the example above, this is at 9:00 a.m.), the remote site automatically initiates a “going online” request to the host PBX. If the MIG RLC successfully receives the request, the remote site and its telephones go online.

Changing the online/offline mode

Whether an online/offline schedule is used or not, you can put the remote site into online or offline mode at any time by dialing one of two special prefix (SPRE) codes at any phoneset at the remote site. The online and offline SPRE codes are configured through using Configuration Manager with a pound prefix (# in North America) so they do not conflict with the dialing plans used at the host PBX.

Variable security

Security is configured on a card-wide basis for each MIG RLC. You configure this information through the Configuration Manager. See “Remote connection configuration” on page 174.

The MIG RLC offers three levels of security. For a detailed description of the MIG RLC’s variable the security levels, see “Meridian Internet Gateway Reach Line Card security” on page 19.

Security levels

Implement one of the following levels of security to protect MIG RLC and remote-site configuration settings:

- no security

  The MIG RLC allows all calls, regardless of source, to access the corporate PBX.

  Note: No security is the default security level.
- caller ID security

  The MIG RLC compares the caller ID of the incoming call against the caller IDs entered for this remote unit through the Configuration Manager. If the caller ID does not match any of those entered in this unit’s Caller ID table, the MIG RLC denies PBX access to this call. For the required steps to configure security level 2 on your MIG RLC, see “Remote connection configuration” on page 174.

- security identifier

  When security identifier is used, the following verification takes place, depending on which unit initiated the call:

  1. If the call is from a remote unit to the MIG RLC, the MIG RLC compares the remote unit's outbound security identifier with the inbound security identifier configured for the remote unit on the MIG RLC.

     If the call is from the MIG RLC to a remote unit, the remote unit compares the MIG RLC's outbound security identifier with the inbound security identifier configured for the MIG RLC on the remote unit.

  2. If the compared identifiers match, the receiving end accepts the call. If the compared identifiers do not match, the receiving end rejects the call.For instructions on how to configure this security level on your MIG RLC, see "Remote connection configuration" on page 174.

Data network security

The MIG RLC does not provide for data network security. If security on the data network is an issue, implement security on the data network devices.

System security

Two layers of security protect the MIG RLC and its remote sites:

- administration password

  The administration password is required when starting the Configuration Manager software. If the person attempting to use the Configuration Manager password does not know the password, that person cannot log on to any MIG RLC-related nodes.

  Note: A MIG RLC-related node is any MIG RLC or remote site connected to the host PBX.

- node password

  Users must enter the node password before the configuration of a particular node can be displayed or modified.

Network considerations

Introduction

When you implement a MIG RLC-based remoting system, consider ways that the new equipment can effect your current telecommunications and data networks.

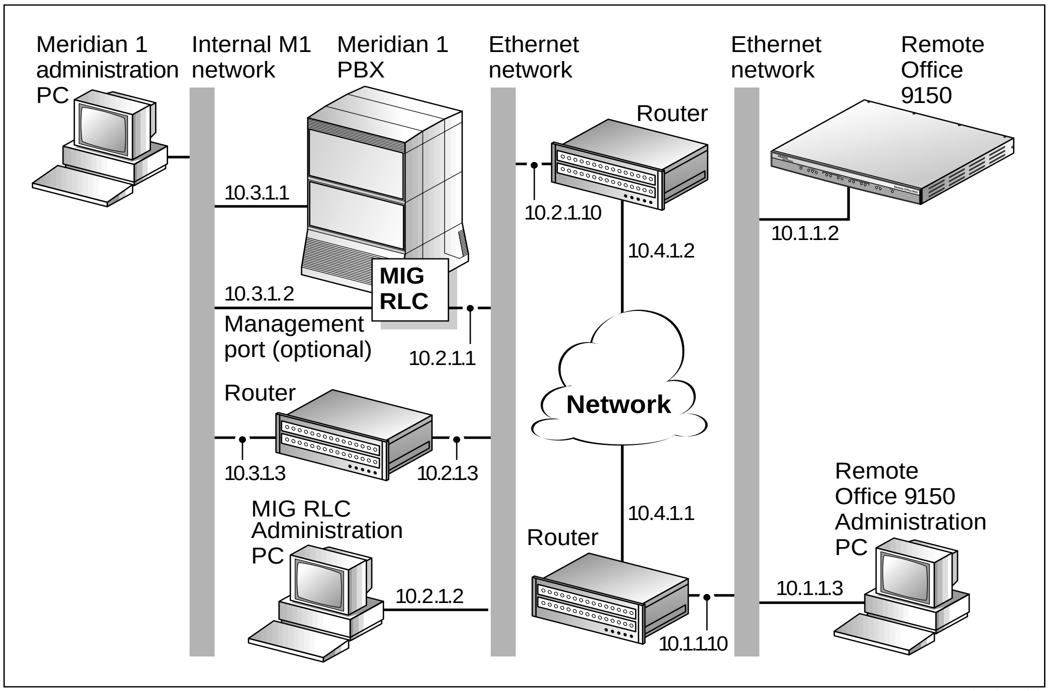
IP addressing and routing

To make and receive calls over the IP network, the MIG RLC must have

- a physical connection to the IP network
- a unique IP address and subnet mask

Network diagram

The following diagram shows the MIG RLC's position in an IP network.



G101400

Quality of Service

The routers used on your IP network must be capable of handling voice traffic with little or no congestion and few delays. If the network is congested or is subjected to many delays, voice quality suffers.

Trunks and dialing plans

Trunk access and SPRE codes used by Remote Office 9150 units are automatically defined in Configuration Manager with a pound sign (# in North America) so that there are no conflicts with host PBX dialing plans.

Call blocking

The voice processing capacity of the system being remoted depends on the number of DSP application and trunk interface modules installed at the host and remote sites. This voice processing capacity defines how many calls can be active at one time and the amount of bandwidth made available to the site.

Reducing call blocking in circuit-switched mode

ISDN BRI trunks are required for a Remote Office 9150 unit to operate in circuit-switched mode (that is, for the Remote Office 9150 unit to operate over the PSTN) instead of the IP network.

At the host location, the only method for reducing call blocking in the circuit-switched mode is to increase the number of trunks available to the MIG RLC.

Reducing call blocking in Voice over IP mode

One DSP application module provides the ability to support eight simultaneous calls when voice traffic is routed over the IP network or over the PSTN. You can install up to four DSP application modules in the MIG RLC.

Calculating system requirements

For help in determining how many DSP application modules you need to reduce or eliminate call blocking, refer to “DSP requirements” on page 39 and the MIG RLC System expansion worksheet on page 338.

Administration PC

Introduction

The administration software is Windows-based and is installed on a PC. This section describes ways that you can connect an administration PC to the MIG RLC. It also describes the hardware and software requirements for using the administration software.

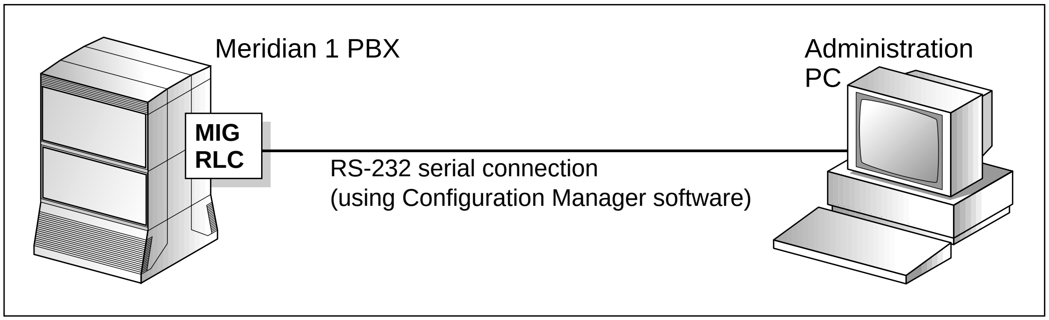
Connection options

The MIG RLC product includes the Configuration Manager software that enables you to configure, administer, and upgrade the MIG RLC. These tasks can be performed over one of the following connections:

- RS-232 serial connection (required for first-time configuration)
- 10BaseT Ethernet connection (for ongoing administration)

Serial connection

Use the serial connection when you first install and configure the MIG RLC. You must establish a serial connection to the MIG RLC to enter the IP interface information, as shown in the illustration below.



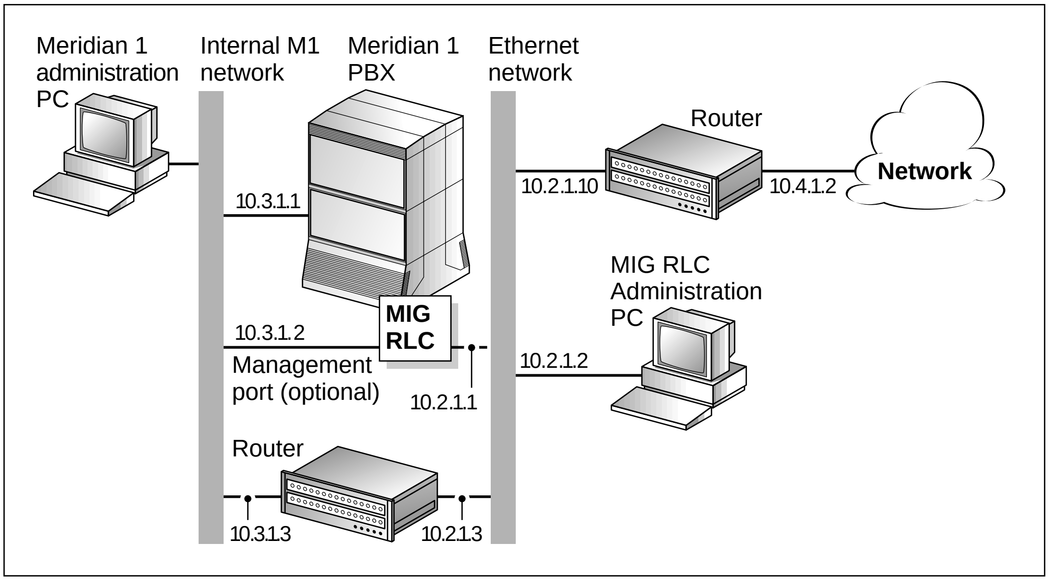
You can continue using the serial connection for ongoing administration of the MIG RLC if you wish. However, if this is the only connection option used, the MIG RLC cannot be administered remotely.

Ethernet connection

Once you have configured the MIG RLC with its IP interface information, the following can happen:

- Calls can be routed between the MIG RLC and remote units.
- You can administer the MIG RLC over the IP network.

  This means you do not have to install an administration PC in the same location as the MIG RLC. See the following diagram.

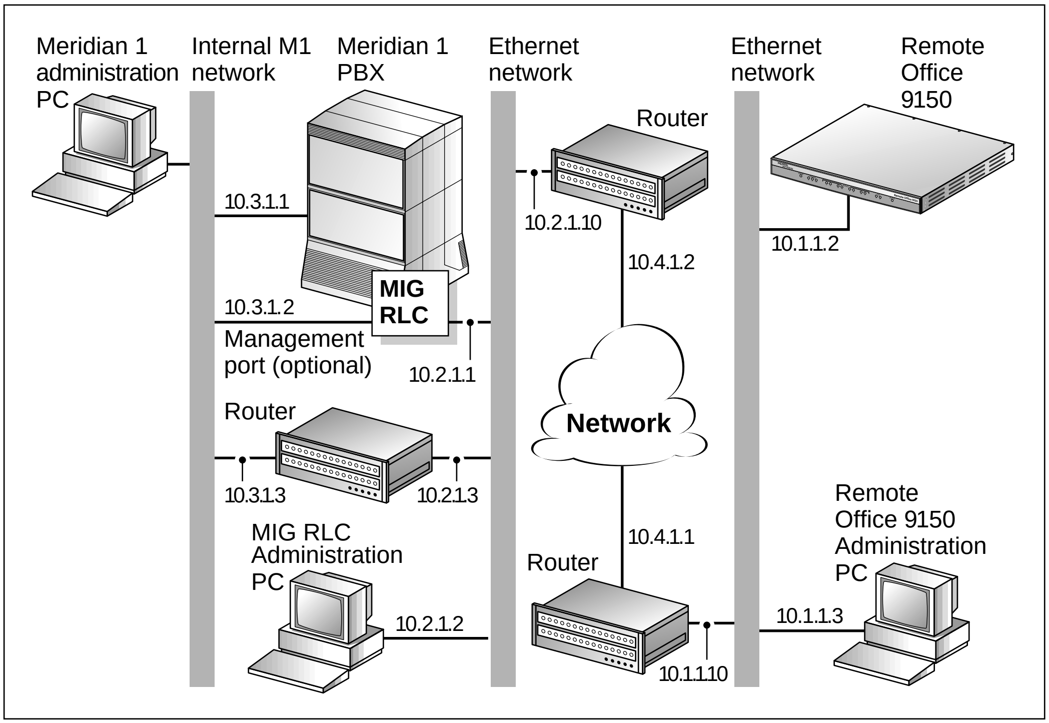


G101414

Administering multiple nodes

If you are responsible for administering the MIG RLC on the host PBX and one or more remote units, you can access the MIG RLC and the remote unit from anywhere on the network. The following diagram shows an example of an assembled network with administration PCs.

Note: You do not have to install separate administration PCs for the MIG RLC and each remote unit.



G101400

Windows PC requirements

To use Configuration Manager, the administration PC must

- be an IBM-compatible PC
- use Windows 95, Windows 98, or Windows NT with the Microsoft TCP/IP networking component installed

  Note: Windows 2000 is not supported.
- be equipped with a CD-ROM drive
- be equipped with a 10BaseT Ethernet interface card (this provides access to the Ethernet network)
- have an available COM port if you want to use the RS-232 serial port to establish a direct serial connection

- be equipped with a pointing device
- use Microsoft's IP stack
- have 32 Mbytes of RAM for Windows 95 and 98, or 64 Mbytes of RAM for Windows NT
- have 48 Mbytes of available storage for Windows 95 and 98, or 64 Mbytes of available storage for Windows NT

Trivial File Transfer Protocol server

The administration PC must have a TFTP server application installed to perform firmware upgrades and configuration uploads. The administrator must know the TFTP server's IP address in the network.

You can use any TFTP server application. These applications are available from the Internet.

Year 2000 compliance

The MIG RLC and Configuration Manager software are Year 2000 compliant. However, ensure the administration PC is Year 2000 compliant by verifying that the Windows operating system is listed in this table:

Operating system	Year 2000 compliance requirement
Windows NT	Service Pack 5
Windows 95	Version 95b
Windows 98	OK as is

Note: Windows 2000 is not supported.

Meridian Administration Tools and Configuration Manager

Meridian Administration Tools (MAT) and Configuration Manager are not guaranteed to operate simultaneously on the same administration PC. Simultaneous running of these two applications has not been tested and is, therefore, not supported.

Planning for future growth

Introduction

The MIG RLC can change as your telecommunication needs change or grow. This section describes planning for these needs.

Basic planning issues

When determining remote channel needs for your network, it is important to consider the number of users and planned growth at each site in the network.

Adding DSP modules

The MIG RLC ships with the ability to support up to eight simultaneous telephone calls.

You can increase the voice processing capability of the MIG RLC by installing up to three DSP application modules. Each DSP application module adds support for up to eight simultaneous calls, for a maximum capacity on a MIG RLC of 40 simultaneous calls.

For instructions on determining how many DSP application modules you need, see the System expansion worksheet on page 338. For instructions on installing additional DSP modules, see “Installing DSP application modules” on page 71.

Deployment options

Introduction

You can install and configure the MIG RLC on the host PBX and remote units to initially use one of the following:

- only the IP network (Voice over IP)
- only the circuit-switched network (for example, ISDN BRI trunks)
- both networks (which allows QoS transitioning technology functionality)

If you choose not to use both networks initially, this section suggests how you can gradually phase in Voice over IP and QoS transitioning technology functionality.

ATTENTION

Even if you plan to route calls over the circuit-switched network only, you must assign an IP address and gateway to the MIG RLC and remote units. This allows you to administer these nodes from an administration PC that is located elsewhere on the network.

Port and station assignment

Regardless of which network you use initially to route calls, you must plan MIG RLC port and remote site user station assignment. For this release, assign each user at the remote site to one MIG RLC port. Use the following forms to plan port and station assignment:

- “Meridian Internet Gateway Reach Line Card Connection Information—16 ports” on page 324
- “Meridian Internet Gateway Reach Line Card Connection Information—32 ports” on page 329
- “Remote Office 9150 Configuration Information—Stations” on page 344

To implement circuit-switched mode

In a network using circuit-switched mode only, the PSTN processes all incoming and outgoing calls

- to or from the host PBX (host-controlled mode)
- to or from other PSTN customers (local-controlled mode)

To use this scenario, you must do the following:

1 Determine how many simultaneous calls you want to process over the circuit-switched network. This helps you to determine how many DSP application modules to install on the MIG RLC.

To do this, complete the MIG RLC System expansion worksheet on page 338.

Similarly, calculate how many trunk interface and DSP application modules must be installed on each Remote Office 9150 unit, using the Remote Office 9150 System expansion worksheet on page 353.

2 Arrange for ISDN BRI lines from the PSTN to each Remote Office 9150 site, if they are not already present.

3 Install DSP application modules on the MIG RLC, if needed.

4 Install ISDN BRI trunk interface and DSP application modules on each Remote Office 9150 unit, if needed. Up to four ISDN BRI modules and up to three DSP application modules may be installed.

Note: The Remote Office 9150 units do not ship with trunk interface modules or DSP application modules installed.

5 Obtain the telephone number assigned to the MIG RLC port to which the remote unit is assigned. Configure this telephone number on the remote unit—the remote unit uses it to establish connections with the MIG RLC.

6 For each Remote Office 9150 unit, obtain the information for each ISDN BRI line from the Remote Office 9150's telephone service provider. Configure this information on the Remote Office 9150 unit to establish the trunk interface with the PSTN.

7 Identify the telephone number assigned to the remote unit. Configure this telephone number on the MIG RLC—the MIG RLC uses it to establish connections with the remote site.

To implement Voice over IP mode

In Voice over IP mode, all incoming and outgoing calls are processed across the IP network to or from the host PBX. Calls that are made to external parties through the host PBX are routed to the PSTN using the host PBX's trunks. Both internal and external calls that are made through the host PBX are referred to as host-controlled calls.

Note: You can implement support for local PSTN calls at each Remote Office 9150 site by adding ISDN BRI lines at that site. Local PSTN calls are referred to as local-controlled calls.

To implement Voice over IP mode for host-controlled calls, you must do the following:

1 Determine how many simultaneous calls you want to process. This helps you to determine how many DSP application modules to install on the MIG RLC. To do this, complete the MIG RLC System expansion worksheet on page 338.

Similarly, to calculate how many DSP application modules to install on the Remote Office 9150 unit (if any), use the Remote Office 9150 System expansion worksheet on page 353.

2 Install DSP application modules on the MIG RLC, if needed.

3 Obtain the IP address assigned for the remote unit. Configure this IP address on the MIG RLC—the MIG RLC uses it to establish connections with the remote unit.

4 Similarly, obtain the IP address assigned to the MIG RLC. Configure this IP address on the remote unit—the remote unit uses it to establish connections with the MIG RLC.

5 If Voice over IP mode is stage 2 in your network implementation, run this stage with a minimal number of users until you are sure that

- your IP network can handle the additional traffic
- you can identify the kinds of configuration adjustments you need to make to the IP network to handle that traffic

When you are satisfied with the IP network performance, continue with QoS transitioning technology implementation.

To implement the Quality of Service transitioning technology

When the QoS transitioning technology is implemented, calls transition

- from the IP network to the circuit-switched network when IP QoS degrades
- back to the IP network from the circuit-switched network when IP QoS returns to normal

1 To implement the QoS transitioning technology, you must understand what your IP network is doing, such as

- when the busy times are on the network
- how much traffic the network processes (during normal and busy traffic periods)
- how to evaluate and adjust your network's QoS

Consult with your data network administrator. Refer also to Appendix A, "Network engineering guidelines," on page 267.

2 Once you understand this information, determine the QoS settings that you want, then configure them on each MIG RLC port.

For instructions, refer to "Configuring Quality of Service" on page 183.

3 If IP mode is the last stage in your network implementation, run this stage with a minimal number of users until you are sure that your IP network's QoS is acceptable.

4 When you are satisfied with QoS transitioning performance, deploy the capability to the entire network.

Chapter 3

Installing the Meridian Internet Gateway Reach Line Card

In this chapter

Overview

Introduction

This chapter contains the procedures you need to

- install your MIG RLC in the host site’s Meridian 1 PBX
- plan and implement growth of remote sites through DSP management

General safety

You can find the general safety guidelines recommended by Nortel Networks on page 69. Follow these guidelines whenever you perform installation or maintenance tasks on MIG RLCs or DSP application modules.

Required tools

You can find a discussion of the tools you need to perform MIG RLC installation and maintenance tasks on page 70.

Identifying the cables

Cable your MIG RLC according to the transport mechanism(s) available to your system. Refer to pages 73 and 74 for descriptions of the cables, including an identification of the connectors on each cable and the connectivity carried by each connector.

Installing the Meridian Internet Gateway Reach Line Card

The process of installing a MIG RLC involves

- preparing the switch
- placing the MIG RLC into its slot
- cabling the MIG RLC

Whether your system consists of one or multiple MIG RLCs, the process is the same for each MIG RLC at the host site. See page 76 for the necessary procedures.

Verifying the installation

After installation, use the verification methods on page 79 to ensure that you have followed the MIG RLC installation procedures properly.

Installing the software

Use the Configuration Manager software to configure and administer the MIG RLC. This software is located on the CD-ROM provided in the package. It must be installed on the administration PC.

See page 80 for the proper procedure.

Using the Configuration Wizard to perform initial configuration

The Configuration Wizard option in Configuration Manager allows you to configure the minimum information needed for establishing communications between the MIG RLC at the host site and the unit at the remote site. The Configuration Wizard does not provide all the configuration settings that are available in Configuration Manager. By using the Configuration Wizard, the MIG RLC can be up and running within ten minutes.

You can use the Configuration Wizard in offline mode or while connected and logged on to the MIG RLC (online mode). See page 82 for the proper procedures.

Installing DSP application modules

Install DSP application modules in the expansion slots on your MIG RLC to increase the number of channels, and thus telephone lines, that you can use at your remote sites. For the necessary procedures, see “Installing DSP application modules” on page 71.

General safety

Introduction

This section describes general safety guidelines recommended by Nortel Networks. Follow these safety guidelines whenever you perform installation or maintenance tasks on the MIG RLC.

Precautionary messages

This guide provides warnings related to hardware installation and handling. For a description of these warnings, see “Conventions used in this guide” on page xxi.

Electrostatic discharge safety precautions

Electrostatic discharge (ESD) affects the performance and decreases the useful life of system components. It can seriously damage DSP application modules and component parts, such as MIG RLCs.

Required tools

Introduction

This section identifies the tools you need to perform MIG RLC installation and maintenance tasks.

Hardware installation tools

You need the following tools to install the MIG RLC or to install or replace DSP application modules:

- antistatic ESD wrist strap (recommended)
- Phillips (cross-head) screwdriver
- slot-head screwdriver
- pen or pencil for
  - noting cable lengths
  - labeling cables
- cable tie wraps
- cable identification labels
- tape measure

Software installation or upgrade tools

In addition, if you are performing a first-time installation or a maintenance upgrade, you need the following items:

- the *Remote Office Product CD-ROM*
- a network connection to the Nortel Networks web site for obtaining upgrade files

Installing DSP application modules

Introduction

Install DSP application modules in the expansion slots on your MIG RLC. This increases the number of channels, and thus telephone lines, that you can use at your remote sites. To add DSP application modules to your MIG RLC, follow these steps:

- Determine the number of DSP application modules that meets your growing needs using the “System expansion worksheet” on page 338.
- Install DSP application modules using the procedure on page 72.

Determining how many DSP application modules to add

Your MIG RLC comes with sufficient DSP resources to provide voice processing for up to eight channels. In addition, DSP expansion slots enable you to add as many as four DSP application modules to your MIG RLC. Each application module increases the voice processing capabilities of your system by up to eight channels.

Note: Non-blocking service requires a one-to-one correspondence of DSP resources at both the host and remote sites.

Use the “System expansion worksheet” on page 338 to determine the number of DSP application modules that your MIG RLC needs to supply enough channels for your remoting needs. Once you have ordered and received the DSP application modules from Nortel Networks, install them according to the procedure found in “To install DSP application modules” on page 72.

Handling DSP application modules

Before beginning the installation and configuration process, review “General safety” on page 69. Follow these safety precautions and warnings to protect your investment in your telecommunications network.

⚠ **CAUTION**

Risk of data loss or equipment damage

Be certain you are properly grounded before handling DSP application modules or the MIG RLC.

To install DSP application modules

1 Ground yourself before handling DSP application modules or the MIG RLC.

2 Clear a flat, static-free work area with sufficient space to hold your MIG RLC and DSP application modules.

3 With the DSP application modules still in their antistatic bags, place them in the work area.

4 Remove the MIG RLC from the PBX.

5 Place the MIG RLC in the work area.

6 Remove a DSP expansion module from its antistatic bag, holding it by the edges, with the insertion tabs facing down.

7 Insert the tabs into a pair of expansion slots on the MIG RLC. (See the illustration on page 5 for the location of expansion slots.) The tabs should snap into place when fully inserted. Visually inspect each tab to make sure that there is no gap and that it is fully inserted.

Identifying the cables

Introduction

Cable your MIG RLC according to the transport mechanism(s) your system uses. The following table identifies the cables available from Nortel Networks according to the transport mechanism connections that your system can access:

IF your system can access	THEN you need the
PSTN and VoIP connections	RLC Multi-I/O cable–Basic (NTDR79xx).
PSTN, local telephones, and VoIP connections	RLC Multi-I/O cable–Enhanced (NTDR80xx).

Pin-out tables for each of these cables are located in Appendix D, “Pin-out tables for RLC Multi-I/O cables.”

RLC Multi-I/O cable–Basic (NTDR79xx)

The RLC Multi-I/O cable–Basic provides connectivity to an Ethernet port for accessing the corporate LAN using Voice over IP (VoIP) signaling and a serial port for maintenance and administrative functions using RS-232 signaling.

The following table describes the cable connectors on the RLC Multi-I/O cable–Basic and the connectivity supplied by each connector:

The connector labeled	is a	that transmits	and connects to the
P1	25-pair connector (female)	all signals	I/O panel.

Note: If you are using a double-wide, 32-channel MIG RLC, insert P1 into the socket for the first of the two card slots occupied by the MIG RLC.

The connector labeled	is a	that transmits	and connects to the
P2	DB-15 connector (male)	10BaseT signaling	CLAN Ethernet (customer LAN on the network).
Note: P2 requires a DB-15 to RJ-45 converter (shipped with the cable).			
P3	DB-9 connector (female)	RS-232 signaling	serial port connection for administration and maintenance.

RLC Multi-I/O cable–Enhanced (NTDR80xx)

You can purchase the RLC Multi-I/O cable–Enhanced separately from Nortel Networks. This cable provides connectivity to an Ethernet port for accessing the corporate LAN using VoIP signaling and a serial port for MMI maintenance and administration functions using RS-232 signaling, like the RLC Multi-I/O cable–Basic.

In addition, this cable provides connection to a second Ethernet port for accessing the switch's internal Ethernet (embedded LAN, or ELAN) using VoIP signaling, and a cross-connect device to local telephones using Time Compression Multiplexing (TCM).

The following table describes the cable connectors on the RLC Multi-I/O cable–Enhanced and the connectivity supplied by each connector:

The connector labeled	is a	that transmits	and connects to the
P1	female 25-pair connector	all signals	I/O panel.
Note: If you are using a double-wide, 32-channel MIG RLC, insert P1 into the socket for the first of the two card slots occupied by the MIG RLC.			

The connector labeled	**is a**	**that transmits**	**and connects to the**
P2	male DB-15 connector	10BaseT signaling	CLAN Ethernet (customer LAN on the network).
Note: P2 requires a DB-15 to RJ-45 converter (shipped with the cable).			
P3	female DB-9 connector	RS-232 signaling	serial port connection for administration and maintenance.
P4	male DB-15 connector	10BaseT signaling	ELAN Ethernet (PBX’s embedded LAN).
Note: P4 requires a DB-15 to RJ-45 converter (shipped with the cable).			
P5	male 25-pair connector	TCM signaling	cross-connect to local telephones.
P6	male DB-25	V.35 signaling	Frame Relay Access Device (FRAD).
Note: P6 is reserved for future use.			

Installing the Meridian Internet Gateway Reach Line Card

Introduction

The process of installing the MIG RLC involves

- preparing the switch
- placing the MIG RLC into its slot
- cabling the MIG RLC

Whether your system consists of one or multiple MIG RLCs, the process is the same for each one.

Preparing for installation

Configure the slot into which the MIG RLC is to be inserted as if it were to hold an extended digital line card (XDLC). Refer to the documentation specific to your switch for the exact procedures.

Split-slot wiring

NT8D37AA IPE cabinets use split-slot wiring. If you have one of these cabinets, your MIG RLCs can only reside in slots 0, 4, 8, and 12 without rewiring the slot. To use any other slot, rewire part of the IPE backplane using cable NT8D81AA (A0359946). Refer to the *Meridian 1 System Installation and Maintenance Manual* (NTP 553-3001-210) for details.

To install a MIG RLC

1. Insert the MIG RLC into its card slot.

   Ensure that the lower tips of the ejector tabs are positioned properly inside the front edges of the shelf.

2 Lock the MIG RLC into position by pushing the handles toward one another until they touch the faceplate.

If you meet with inappropriate resistance, stop and reposition the card.

See “LED indicators” on page 7 for the sequence of events that signify a successful MIG RLC installation.

3 Verify that the switch recognizes the presence of the MIG RLC. (Refer to the documentation specific to your switch for exact procedures.)

To cable a MIG RLC

1 Plug P1 of the RLC Multi-I/O cable (Basic or Enhanced), the 25-pair connector, into the 25-pair shelf connector associated with the slot occupied by the MIG RLC.

Note: If you are cabling a 32-channel MIG RLC, use the shelf connector associated with the first of the two slots occupied by the MIG RLC.

2 Plug P2, the male DB-15 connector (if using the Enhanced cable, this is the first male DB-15 connector) into a DB-15 to RJ-45 adapter (NT7R93CA).

Notes:

- This adapter is supplied with the RLC Multi-I/O cable–Enhanced.
- This adapter is *not* an active transceiver.

a. Plug one end of a CAT5 data cable of a sufficient length to reach your Ethernet hub into the other side of the DB-15 to RJ-45 adapter connected to P2.

b. Plug the other end of the CAT5 data cable into your Ethernet hub.

3 Plug P3, the female DB-9 connector of the RLC Multi-I/O cable (Basic or Enhanced), into the Remote Office administration PC.

Note: The preceding steps apply to both the RLC Multi-I/O cable–Basic and the RLC Multi-I/O cable–Enhanced.

- If you are using the RLC Multi-I/O cable–Basic (NTDR79xx), proceed to “Verifying the installation” on page 79.
- If you are using the RLC Multi-I/O cable–Enhanced (NTDR80xx), proceed to step 4.

4 Plug P4, the second male DB-15 connector of the RLC Multi-I/O cable–Enhanced, into a DB-15 to RJ-45 adapter (NT7R93CA).

Notes:

- This adapter is supplied with the RLC Multi-I/O cable–Enhanced.
- This adapter is *not* an active transceiver.

a. Plug one end of a CAT5 data cable into the DB-15 to RJ-45 adapter connected to P4.

b. Plug the other end of the CAT5 data cable into the I/O panel connector corresponding with the switch's Input/Output Port (IOP) card.

5 Plug P5, the second 25-pair connector, into the cross-connect device serving the local telephones you want to attach to MIG RLC ports not needed for remoting purposes.

6 P6 is reserved for future use.

Verifying the installation

Introduction

Once you have finished the host-site installation and cabling of your MIG RLC system, verify that you have completed these procedures properly.

Indications of proper installation

When a MIG RLC is placed in its slot, it automatically performs a self-test. A successful self-test indicates proper installation. The following behaviors by the Maintenance LED confirm a successful self-test:

- blinking three times
- turning off (if enabled by the switch)
- remaining off (if enabled by the switch)

Note: See “LED indicators” on page 7 for a further explanation of LED behavior at startup.

Indications of proper cabling

The ability to successfully log on to the MIG RLC using Configuration Manager indicates proper cabling of the MIG RLC. To perform this task, install the software first (see page 80). Once this task is completed, see “To start Configuration Manager” on page 83.

What to do if you cannot log on to the MIG RLC

If you are not able to log on to the MIG RLC using Configuration Manager, confirm that the MIG RLC is cabled properly before attempting troubleshooting procedures.

Note: If the MIG RLC is cabled properly and you still cannot log on, see Chapter 8, “Troubleshooting.”

Installing the software

Introduction

Use the Configuration Manager software to configure and administer the MIG RLC. This software is located on the CD-ROM provided in the package. You must install it on the administration PC.

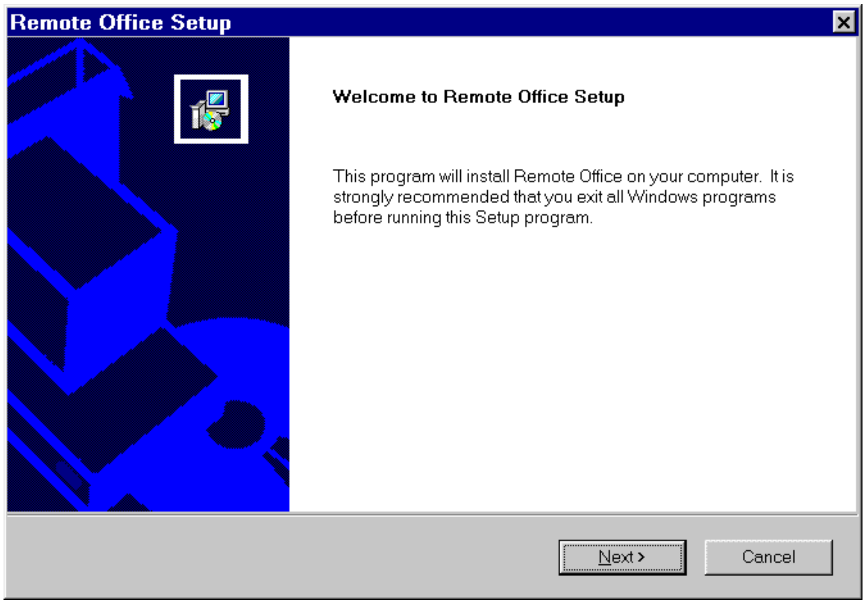
To install the software

1 Insert the CD-ROM in the applicable drive.

Result: If autorun is enabled on your PC, a Welcome screen appears listing available options.

2 If autorun has started, select the Install option; otherwise, locate and double-click setup.exe (located in the Software directory on the CD-ROM).

Result: The InstallShield prepares for installation, and then the Welcome screen appears.



Welcome to Remote Office Setup

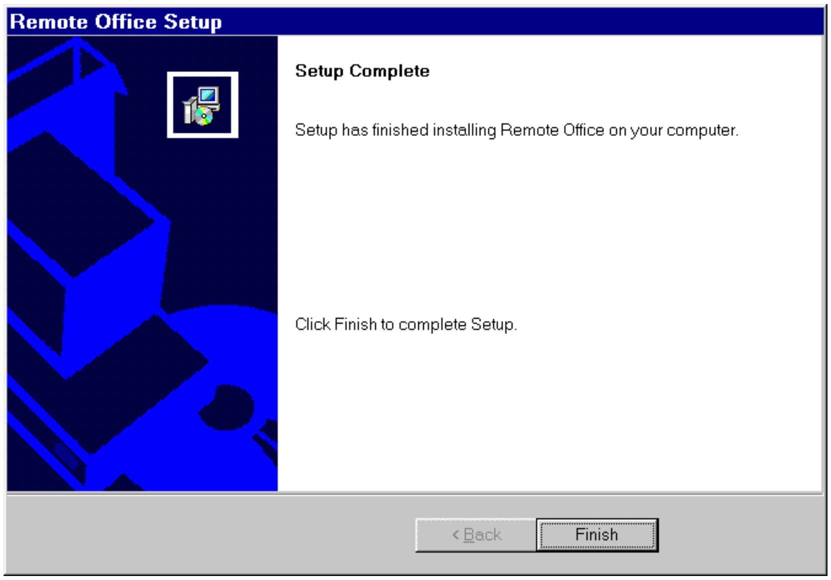
This program will install Remote Office on your computer. It is strongly recommended that you exit all Windows programs before running this Setup program.

3 Click Next, then follow the screen prompts.

Result: Once the software has been installed, messages appear confirming that the Windows registry has been updated and that the installation was successful.

4 Click OK to both messages.

Result: The Setup Complete screen appears.



Setup Complete

Setup has finished installing Remote Office on your computer.

Click Finish to complete Setup.

Note: You might be prompted to restart your computer. If you are, then click Yes, I want to restart my computer.

5 Click Finish.

What's next?

After you install the software on the administration PC, start Configuration Manager and run the Configuration Wizard. The Configuration Wizard allows you to perform initial configuration quickly and easily.

For instructions, see "Using the Configuration Wizard to perform initial configuration" on page 82.

Note: Leave DLL files installed by the Configuration Manager InstallShield in the Windows system directory. Do not move these files to any other directory.

Using the Configuration Wizard to perform initial configuration

Introduction

The Configuration Wizard option in Configuration Manager allows you to configure the minimum information needed for establishing communications between the MIG RLC at the host site and the Remote Office 9150 unit at the remote site. The Configuration Wizard does not provide all the configuration settings that are available in Configuration Manager. By using the Configuration Wizard, the MIG RLC can be up and running within ten minutes.

You can use the Configuration Wizard in offline mode or while connected and logged on to the MIG RLC (online mode).

What you can configure with the Configuration Wizard

The Configuration Wizard allows you to configure the following elements:

- the MIG RLC’s IP address, subnet mask, and default gateway

  This information must be valid for your IP network.

  Note: If you will not be using the IP network to route calls, you must still enter this information for administration purposes. If you do not have an IP network in place, sample information is provided in the procedure on page 87.
- for Voice over IP capability: the IP addresses for each remote unit to which the MIG RLC connects
- for circuit-switched network capability:
  - the MIG RLC port to be used for connection to the remote unit
  - the telephone number of the remote unit

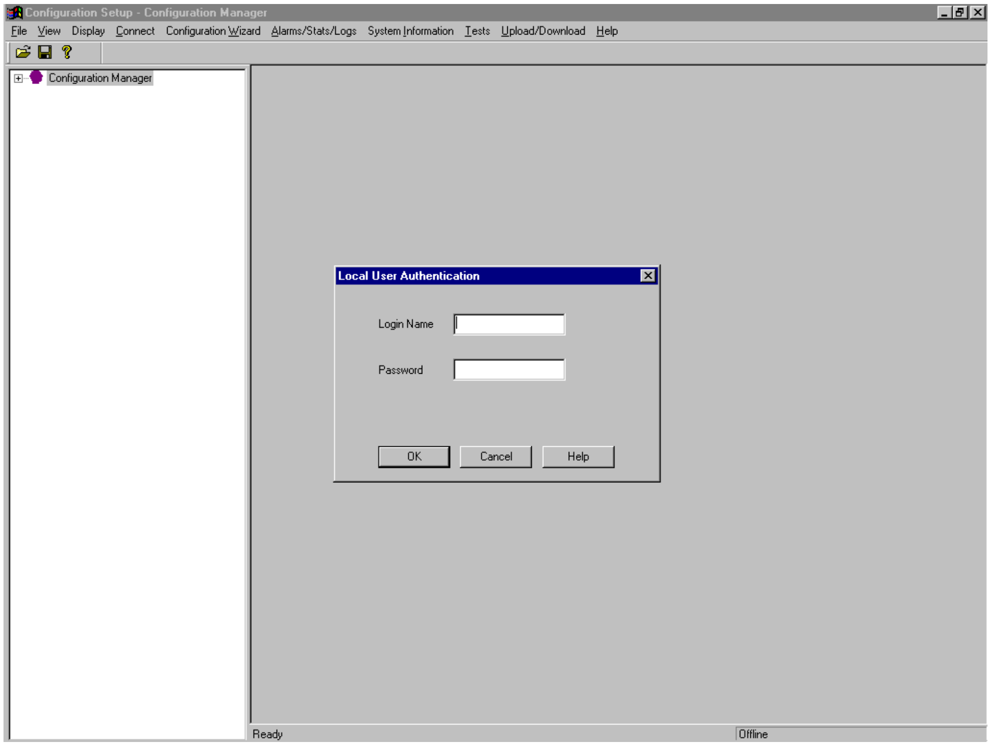
Ensure you have this information ready before you begin.

Note: If, after completing configuration with the Configuration Wizard, you want to modify any settings, you must use the Configuration Manager.

To start Configuration Manager

1 Click Start → Programs → Remote Office → Configuration Manager.

Result: The Configuration Manager opens and you are prompted for the logon name and password.

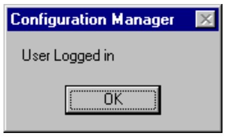

Configuration Setup - Configuration Manager
File View Display Connect Configuration Wizard Alarms/Stats/Logs System Information Tests Upload/Download Help
Configuration Manager
Local User Authentication
Login Name
Password
OK
Cancel
Help
Ready
Offline

2 Type **admin** in to the Login Name box.

3 Type **root** in to the Password box.

4 Click OK.

Result: You are informed if the logon was successful.



User Logged in

5 Click OK.

Result: The logon status dialog box disappears.

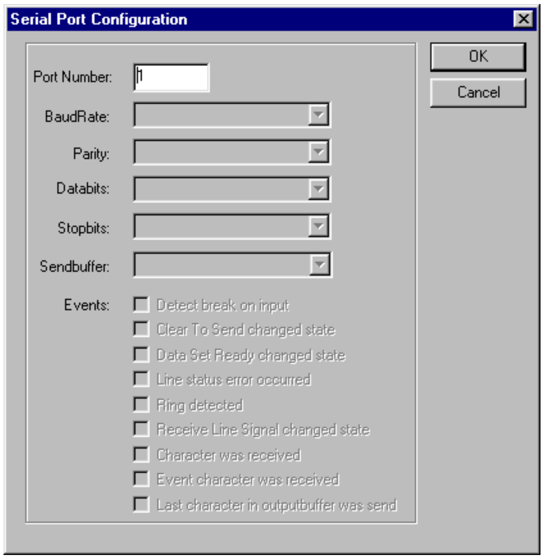
6 Do one of the following:

IF you want to perform an	THEN
offline configuration	■ Choose View → Device Type → RLC. ■ Continue with “To perform configuration with the Configuration Wizard” on page 87.
online configuration	continue with “To establish a serial connection” on page 84.

To establish a serial connection

1 From the menu, choose Connect → Login board → Serial.

Result: The Serial Port Configuration dialog box appears.



Serial Port Configuration

Port Number: 1

BaudRate:

Parity:

Databits:

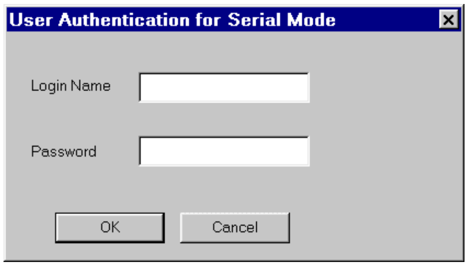
Stopbits:

Sendbuffer:

Events:
- □ Detect break on input
- □ Clear To Send changed state
- □ Data Set Ready changed state
- □ Line status error occurred
- □ Ring detected
- □ Receive Line Signal changed state
- □ Character was received
- □ Event character was received
- □ Last character in outputbuffer was send

2 Enter the COM port number to which the unit is connected, and then click OK.

Result: The User Authentication for Serial Mode dialog box appears.



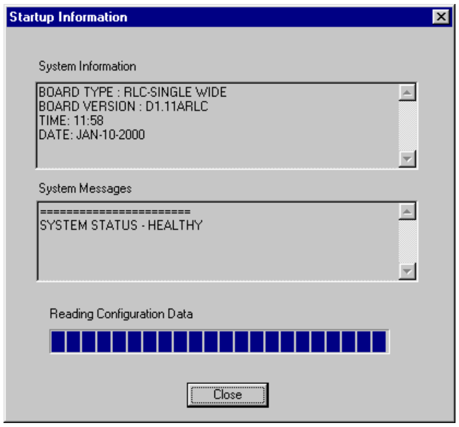
3 Type **guest** for the logon name.

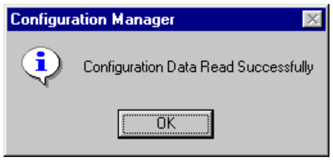
4 Type **guest123** for the password.

Note: This is the default password. It might be different if it was changed.

5 Click OK.

Result: The connection attempt is initiated. The message `Trying to Connect via Serial Port <port number>` might appear.

IF the logon attempt	THEN
failed	the following message appears: `SERIAL CONNECTION FAILED` Go back to step 1.
succeeded	the User Logged In dialog box appears. Click OK. **Result:** The following dialog box appears:  Startup Information System Information BOARD TYPE : RLC-SINGLE WIDE BOARD VERSION : D1.11ARLC TIME: 11:58 DATE: JAN-10-2000 System Messages ====================== SYSTEM STATUS - HEALTHY Reading Configuration Data Close

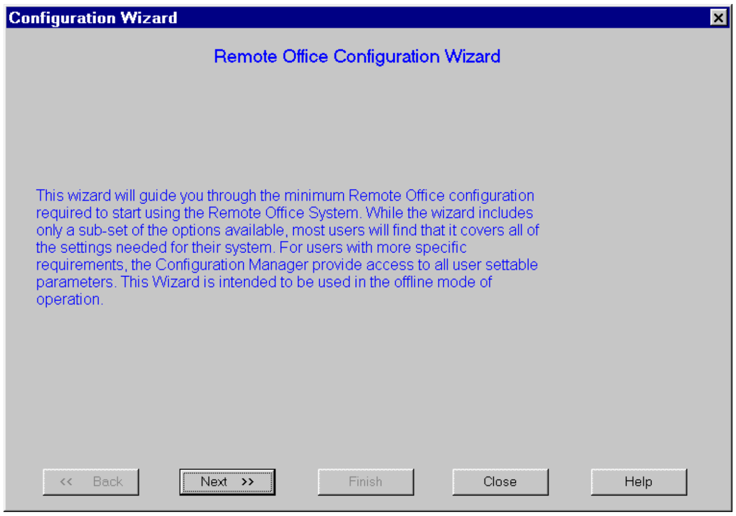
IF the logon attempt	THEN
succeeded (continued)	The following messages appear above the progress bar at the bottom of the dialog box: ■ Reading Hardware Information ■ Reading DSP Load Data ■ Reading Configuration Data These messages mean that Configuration Manager is obtaining the unit’s configuration information from flash memory. When initialization is completed, the following dialog box appears:  Configuration Data Read Successfully Click OK.

To perform configuration with the Configuration Wizard

Note: The screen examples shown in this procedure use information from the sample network diagram on page 359.

1 Choose Configuration Wizard from the menu.

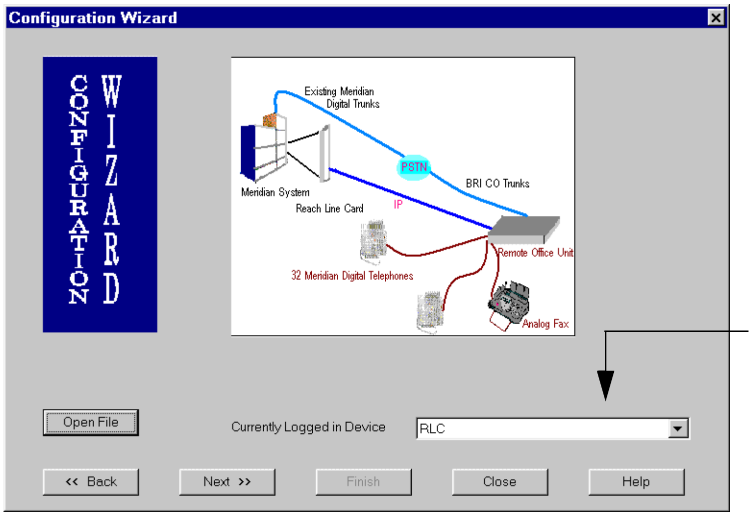
Result: The following screen appears:



This wizard will guide you through the minimum Remote Office configuration required to start using the Remote Office System. While the wizard includes only a sub-set of the options available, most users will find that it covers all of the settings needed for their system. For users with more specific requirements, the Configuration Manager provide access to all user settable parameters. This Wizard is intended to be used in the offline mode of operation.

2 After reviewing the message, click Next.

Result: The following screen appears:



Currently Logged in Device: RLC

Ensure the Device box shows RLC.

3 Verify that the Currently Logged in Device box shows RLC, and then click Next.

If it does not show RLC, select RLC from the list box.

Result: The Local Unit Configuration screen appears.

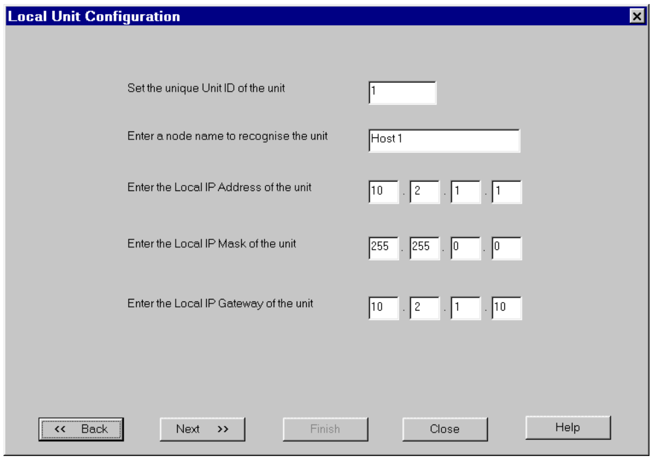
Note: A completed example is shown on page 89.

4 Complete the fields on this screen as described in the following table:

Field	Description
Set the unique Unit ID of the unit	Assign a number from 1–255 to the MIG RLC you are configuring. **Note:** The unit ID assigned to the MIG RLC must be unique from the unit IDs assigned to remote units that connect to this MIG RLC. This implies that different MIG RLCs in the network can have the same unit ID.
Enter a node name to recognize the unit	Enter a name that describes the MIG RLC you are configuring.

Field	Description
Enter the Local IP Address of the unit	Enter the IP address assigned to the MIG RLC. **Note:** If you do not have a valid IP address, type the sample IP address: **10.2.1.1**.
Enter the Local IP Mask of the unit	Enter the subnet mask. **Note:** If you do not have a valid subnet mask, type the sample subnet mask: **255.255.0.0**.
Enter the Local IP Gateway of the unit	Enter the IP address of the gateway between the MIG RLC and the network. **Note:** If there is no router between the MIG RLC and the network, then the administration PC acts as the gateway. Type **10.2.1.10**. ■ as the IP address on the administration PC ■ as the gateway on the MIG RLC

The following is a completed example:



Local Unit Configuration

Set the unique Unit ID of the unit: 1

Enter a node name to recognise the unit: Host 1

Enter the Local IP Address of the unit: 10 . 2 . 1 . 1

Enter the Local IP Mask of the unit: 255 . 255 . 0 . 0

Enter the Local IP Gateway of the unit: 10 . 2 . 1 . 10

The IP information allows you to administer the MIG RLC from any location on the network.

5 Click Next.

Result: The Set the Remote Unit information screen appears.

Note: A completed example is shown on page 91.

6 Complete the fields on this screen as described in the following table:

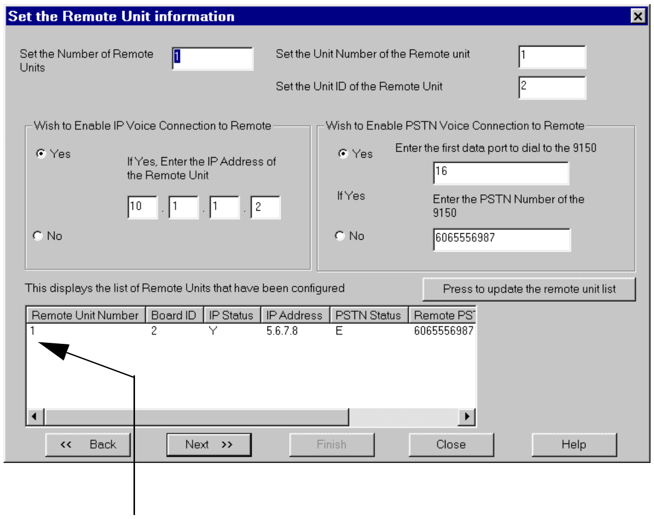
Field	Description
Set the Number of Remote Units	Enter the number of remote units that will be connected to this MIG RLC.
Set the Unit Number of the Remote unit	Enter the number that uniquely identifies the remote unit record you are configuring. **Note:** Each unit that is connected to the same MIG RLC must be given a unique unit record number. This number must not be confused with the unit ID (described below).
Set the Unit ID of the Remote Unit	Assign the number from 1–255 that uniquely identifies the Remote Office 9150 unit to the MIG RLC. This number must be different from ■ the number assigned to the MIG RLC to which this Remote Office 9150 unit connects ■ the numbers assigned to other units connected to the same MIG RLC
Wish to Enable IP Voice Connection to Remote	■ Accept Yes if the IP network will be used to route calls. Then, enter the IP address assigned to the remote unit. ■ Click No if the IP network will not be used. The IP Address boxes are dimmed.
Wish to Enable PSTN Voice Connection to Remote	■ Accept Yes if the circuit-switched network will be used to route calls. Then do the following: **a** Enter the number of the MIG RLC port that is being dedicated for connections to this remote unit. **Note:** The port must be a PBX data port.

Field	Description
Wish to Enable PSTN Voice Connection to Remote (continued)	**b** Enter the telephone number that must be dialed to connect to the remote unit. The telephone number can include the following digits or characters: 0 through 9, #, *, comma (,), period (.), and dash (-). ■ Caller ID separator: “.” (period) ■ Caller ID separator and 1/2 second delay: “,” (comma) ■ null separator: “-” (dash) ■ Click No if the circuit-switched network will not be used. The PSTN Voice Connection boxes are dimmed.

7 Click Press to update the remote unit list.

Result: The information entered for this remote unit appears in the list of configured remote units in the lower half of the screen.

The following is a completed example:


Set the Remote Unit information
Press to update the remote unit list
<< Back
Next >>
Finish
Close
Help

Set the Number of Remote Units: 1

Set the Unit Number of the Remote unit: 1

Set the Unit ID of the Remote Unit: 2

Wish to Enable IP Voice Connection to Remote: ● Yes ○ No

If Yes, Enter the IP Address of the Remote Unit: 10 . 1 . 1 . 2

Wish to Enable PSTN Voice Connection to Remote: ● Yes ○ No

If Yes

Enter the first data port to dial to the 9150: 16

Enter the PSTN Number of the 9150: 6065556987

This displays the list of Remote Units that have been configured

Remote Unit Number	Board ID	IP Status	IP Address	PSTN Status	Remote PS
1	2	Y	5.6.7.8	E	6065556987

Click Yes to allow voice calls over IP, and then enter the Remote Office 9150 unit’s IP address.

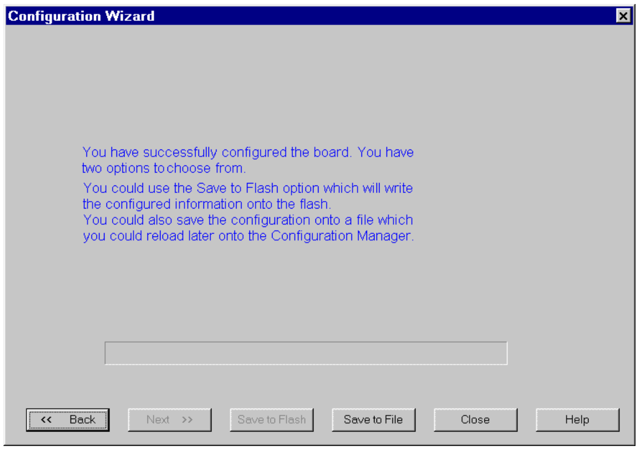
Click Yes to allow voice calls over the circuit-switched network, and then enter the Remote Office 9150 unit’s phone number.

This table allows you to configure connections for more than one remote unit.
To remove an entry from the table, right-click the Remote Unit Number to display the Remove Remote Unit popup, and then left-click to complete the deletion.

8 Repeat steps 6 and 7 for each remote unit you need to configure.

9 Click Next.

Result: The following screen appears:



You have successfully configured the board. You have two options to choose from.
You could use the Save to Flash option which will write the configured information onto the flash.
You could also save the configuration onto a file which you could reload later onto the Configuration Manager.

10 Do one of the following:

IF you are performing an	THEN
offline configuration	**1** Click Save to File. **Result:** You are prompted to specify the directory path and file name for the configuration file. **2** Specify the directory path and file name for this configuration. **Note:** The file name is automatically defaulted with the name you entered as the node name. **3** Ensure the Files of type box shows Text File(*.TXT).

IF you are performing an	THEN
offline configuration (continued)	**4** Click Save to complete the Save to File. **Result:** The file is saved, and then you are asked if you want to configure another board. If you do, click Yes and continue with step 3 on page 88. The information in this file can be opened in Configuration Manager, and then sent and saved in the MIG RLC's flash memory at another time. For instructions, refer to "Working with configuration files" on page 131.
online configuration	**1** Click Save to Flash. **Result:** The information entered is written to the flash memory of the MIG RLC that you are configuring. If successful, the following message appears: `Data Sent Successfully` **Note:** Nortel Networks recommends that you also save the configuration to a file. For instructions on how to do this with Configuration Manager, see "Working with configuration files" on page 131. **2** Restart the MIG RLC.

What's next?

Now that you have configured the minimum information required for network connectivity, you can do the following tasks:

- Test the network connections. For instructions, see "Testing the connections" on page 94.
- Perform additional configuration, if needed. For instructions, see Chapter 6, "Configuring the Meridian Internet Gateway Reach Line Card."

Testing the connections

Introduction

Test the connections to the MIG RLC using the following methods:

1. Check your system's host-site connections to ensure basic PSTN and IP Network connectivity.
2. Perform a PING test. To do this test, the MIG RLC must be physically connected to the IP network.

Check host site connections

When testing the connections in your remote network, you must first confirm that the equipment connections at the host site are all good.

To confirm your telephone network connections

Check the following points in your telephone network connection:

1 Confirm that the proper connections are made for the digital telephones at the cross-connect system in your corporate switch room.

2 Confirm that the RJ-11 plug of the telephone wire leading to the digital telephone is properly and securely seated in the RJ-11 jack in the wall.

3 Confirm that the RJ-11 plug at the other end of the telephone wire is properly and securely seated in the RJ-11 jack at the base of the digital telephone.

If you are using the RLC Multi-I/O cable–Enhanced, check the following points, in addition to those mentioned above:

4 Confirm that the 25-pair connector of Plug 5 and the 25-pair connector of a cable leading to your cross-connect system are properly and securely joined.

5 Confirm that the 25-pair connector at the other end of the cable mentioned in the previous step is properly and securely joined to the 25-pair socket of the cross-connect system.

6 Ensure that the cable leading from the MIG RLC to the cross-connect system is in good condition, end-to-end.

Ethernet connection

Check the following points in your Ethernet connection:

1 Confirm that the DB-15 to RJ-45 adapter at Plug 2 of the RLC Multi-I/O cable–Enhanced is properly and securely joined to Plug 2.

2 Confirm that the RJ45 plug of a CAT5 data cable leading to your Ethernet hub is properly and securely seated in the RJ-45 socket of the DB-15 to RJ-45 adapter discussed in the previous step.

3 Confirm that the other end of the CAT5 data cable discussed in the previous step is properly and securely seated in the appropriate Ethernet hub socket.

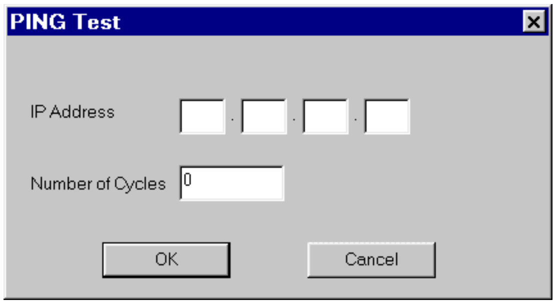
4 Confirm that the CAT5 data cable leading to your Ethernet network's data router is properly and securely seated in the appropriate Ethernet hub socket.

5 Confirm that the CAT5 data cable leading from your Ethernet hub is properly and securely seated in the data router's socket.

To perform a Configuration Manager ping

1 From the menu, choose Tests → Ping.

Result: The PING Test dialog box appears.



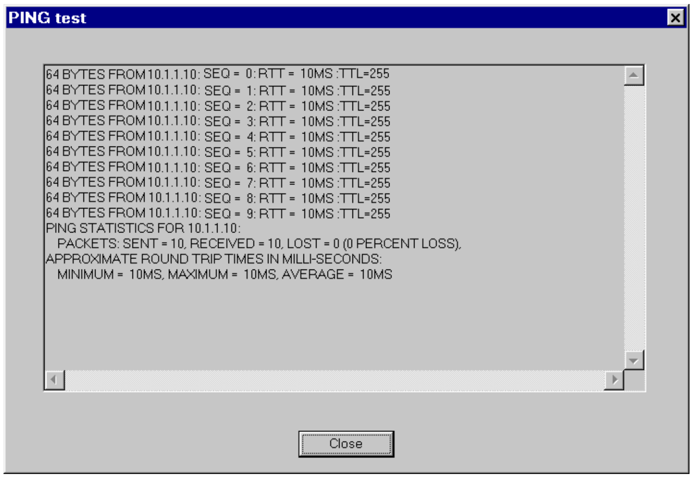
2 Enter the IP Address of the unit you want to ping.

3 In the Number of Cycles box, enter the number of times you want to ping the unit.

The number must be in the range of 1–100.

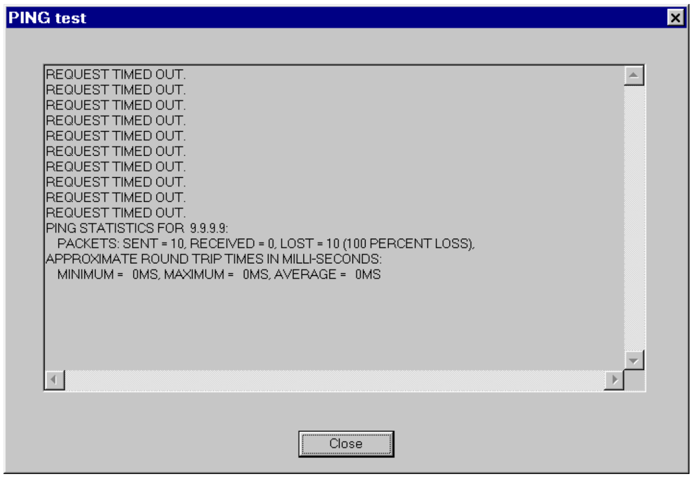
4 Click OK.

Result: The PING test results screen appears, showing the ping results. The following is an example of a successful ping:



```
64 BYTES FROM 10.1.1.10: SEQ =  0: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  1: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  2: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  3: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  4: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  5: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  6: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  7: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  8: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  9: RTT =  10MS :TTL=255
PING STATISTICS FOR 10.1.1.10:
  PACKETS: SENT = 10, RECEIVED = 10, LOST = 0 (0 PERCENT LOSS),
APPROXIMATE ROUND TRIP TIMES IN MILLI-SECONDS:
  MINIMUM =  10MS, MAXIMUM =  10MS, AVERAGE =  10MS
```

The following is an example of an unsuccessful ping:



```
REQUEST TIMED OUT.
REQUEST TIMED OUT.
REQUEST TIMED OUT.
REQUEST TIMED OUT.
REQUEST TIMED OUT.
REQUEST TIMED OUT.
REQUEST TIMED OUT.
REQUEST TIMED OUT.
REQUEST TIMED OUT.
REQUEST TIMED OUT.
PING STATISTICS FOR  9.9.9.9:
  PACKETS: SENT = 10, RECEIVED = 0, LOST = 10 (100 PERCENT LOSS),
APPROXIMATE ROUND TRIP TIMES IN MILLI-SECONDS:
  MINIMUM =   0MS, MAXIMUM =   0MS, AVERAGE =   0MS
```

5 Click Close.

Result: The Ping test screen closes.

What to do if the ping test did not work

1. Ensure you have entered the IP address, subnet mask, and default gateway correctly.
2. PING the gateway to see if it responds.
3. If the PING still does not work, contact your data network administrator.

What's next?

Once you have confirmed that the MIG RLC can be recognized on the network, you can begin to configure it. Nortel Networks recommends that you also change the passwords for logging on to the Configuration Manager and the MIG RLC.

For a description of Configuration Manager, see “Configuration Manager description” on page 115. For the procedure necessary to change passwords, see “Changing the administration password” on page 198.

Chapter 4

Configuring the PBX for the Meridian Internet Gateway Reach Line Card

In this chapter

Overview

Introduction

When you configure a Meridian 1 PBX for a Meridian Internet Gateway Reach Line Card (MIG RLC) system, you must configure three areas:

- trunks
- slots
- ports

Configuring the host trunk

For service providers to properly configure the host trunk for a MIG RLC system, you must tell them the type of ISDN connection (PRI or BRI) you need and what parameters to configure, such as caller ID. In some situations, under strict limitations, a T1/E1 trunk may be used.

Configuring a Meridian Internet Gateway Reach Line Card slot

For the PBX to communicate properly with the MIG RLC, it must recognize it as an extended digital line card (XDLC). This requires that each card slot occupied by a MIG RLC be configured at the PBX as an XDLC card slot.

Understanding port relationships

A fully functioning MIG RLC system requires the interoperation of MIG RLC remote ports, MIG RLC network ports, and remote device ports.

Configuring the host trunk

Introduction

For your service provider to properly configure the host trunk for the MIG RLC, specify which type of ISDN connection (PRI or BRI) you need and what parameters to configure.

Note: BRI trunking is not available in North America.

Recommended trunks

ISDN PRI trunks are the recommended trunks for a MIG RLC.

ISDN PRI configuration

ISDN PRI trunks are used to transport calls between the host PBX and the PSTN. To ensure full functionality for all remote sites served by each MIG RLC, verify with your service provider that the following elements are configured on each trunk:

- two-way voice and two-way data capability
- Caller ID (allows for the selection of Level 2 - Caller ID, for the MIG RLC security level)
- end-to-end digital circuitry, no analog segments (check with both long distance and local service providers)
- non-blocking configuration (ensure that configuration will not block remote site traffic)
- 64 Kbps clear channel

ISDN BRI configuration

Some locations might require ISDN BRI service from the Meridian 1 PBX (the host trunk connection) instead of PRI for geographical reasons. ISDN BRI configuration is identical to ISDN PRI configuration so that, if your host trunk configuration must be BRI, the same configuration elements are needed to ensure full functionality for all remote sites served. Verify this with your service provider.

Note: In North America, an ISDN BRI line can only be ordered as a subscriber line and, therefore, it cannot be used as a trunking option.

Configuring a Meridian Internet Gateway Reach Line Card slot

Introduction

For the PBX to communicate properly with the MIG RLC, it must recognize each MIG RLC as an extended digital line card (XDLC). This requires that each card slot occupied by a MIG RLC be configured at the PBX as an XDLC slot.

Note: You can configure a slot either before or after the card is inserted into the PBX.

To configure a MIG RLC slot

To configure a MIG RLC slot, access the PBX through your PBX administration terminal. At the PBX administration terminal, instruct the PBX to recognize the slot in which the MIG RLC resides as an XDLC slot. Refer to the documentation for your PBX to complete this procedure.

Understanding port relationships

Introduction

This section focuses on the relationship between the two principle MIG RLC ports in a system using the circuit-switched network:

- remote ports
- network ports

ATTENTION

This section is critical to understanding the operation of the Meridian Internet Gateway Reach Line Card.

Functionality provided by the various port types

You can configure ports on the MIG RLC as one of the following:

- a local port

  Local ports support local telephones connected to the host PBX.
- a remote port

  Remote ports support digital telephones on remote units for host-controlled calls. The PBX features and DNs assigned to the MIG RLC ports are the PBX features and DNs available to the remote telephones.
- a network port

  Network ports make and receive PSTN calls to a remote device. Network ports require only the most basic configuration on the PBX that allows this port to place and receive calls of the appropriate type for the particular remote unit. MIG RLC network ports cannot use PBX features such as conference or call forward.

Remote ports

At the host site, the remote ports provide all PBX features and DN assignments for the remote devices on the remote units. The remote ports must be the proper type (voice or data) to match the type of remote device supported by the remote unit.

- Set up digital telephones and the built-in analog port of the Remote Office 9150 unit as voice ports on the host PBX.
- Set up MCAs supported by the MIG RLC as data ports on the host PBX.
- If you have enough data ports available, set up ATAs supported by the MIG RLC as data ports on the host PBX. If you do not have enough data ports available, you can set up ATAs as voice ports on the host PBX.

Network ports

At the host site, the network ports provide the circuit-switched network connections between the MIG RLC and the Remote Office 9150 unit. On the host PBX, configure network port connections to Remote Office 9150 units as data ports.

- If the IP network is the only connection type between the MIG RLC and its remote units, you do not need to configure network ports for the MIG RLC. The communication path between the MIG RLC and the remote unit is an IP path.
- If your system uses both the IP and circuit-switched network connections to route calls, configure a sufficient number of network ports for the MIG RLC to handle the anticipated traffic between the remote unit and the host PBX.

When Quality of Service on the IP network falls below a threshold you configure using the Configuration Manager, the QoS transitioning technology shifts communication from an IP path to a path provided by the network ports. See “Configuring Quality of Service” on page 183 for information on configuring these thresholds.

Configuring remote and network ports

Introduction

Remote and network port configuration is required for MIG RLC operation. You must configure a remote port for each remote device, such as a digital telephone, to be supported by the MIG RLC and at least one network port for each remote unit. A single MIG RLC can support a maximum of four Remote Office 9150 units. However, the same MIG RLC must serve every port on a single remote unit. You cannot assign some ports from one Remote Office 9150 unit to one MIG RLC and other ports from the same unit to another MIG RLC.

Each network port provides 64 Kbps of PSTN bandwidth to a Remote Office 9150 unit. To provide 256 Kbps of bandwidth between the MIG RLC and a Remote Office 9150 unit, configure four network ports. Configuration of remote and network ports takes place at your PBX administration terminal using procedures found in the sections of your PBX's documentation concerning voice and data ports.

Remote port configuration

On your Meridian 1 PBX, configure the remote port according to the telephone at the remote site, with all the features (for example voice mail and call transfer) that you want to access on that telephone.

Network port configuration

Configure the network ports on the MIG RLC as MCA data adapters with the first line able to make and receive data calls. To configure data ports as MCA adapters, make the following settings in LD 11:

Meridian 1 software release	Setting
15–17	CLS prompt = DTA
18 and above	DTA0 prompt = MCA

For further details, refer to the section on LD 11 in the *Meridian 1 X11 I/O Guide* (NTP 553-3001-400).

How the remote and network ports work together

If a phone call is placed to voice port 0 on a completed system, the MIG RLC places a call to the remote site using the dedicated network port for that remote unit. Each network port supports up to eight simultaneous calls. (Confirm that the network port is configured to place calls.) If the MIG RLC status is then queried from the SDI port, the voice port and the selected network port both appear busy.

Note: Each network channel can support as many as eight simultaneous calls.

To configure remote and network ports

At your PBX administration terminal, configure voice ports to the appropriate MIG RLC remote channels supporting remote digital sets and ATAs. Configure data ports to the appropriate MIG RLC remote channels supporting remote MCAs. Configure a network port for every 64 Kbps of bandwidth desired over the PSTN. Configure data ports for each network port supporting a Remote Office 9150 unit.

See PBX documentation for exact procedures and a complete list of possible settings for voice and data ports.

Chapter 5

Configuration Manager overview

In this chapter

Overview

Introduction

Configuration Manager is the software application used to configure and administer the Remote Office 9150 unit and the MIG RLC port to which it is connected.

Viewing the main screen

The main screen is divided into three parts—a menu and two panes.

- The menu across the top of the screen lists various administrative tasks you can perform. These tasks are common to all Remote Office units.
- The pane on the left lists the property sheets you can work with. In this guide, the left pane is called the *system tree*.
- The pane on the right displays the screen associated with an item you selected from the system tree. In this guide, the right pane is called the *property sheet*.

Configuring a unit

You can configure a unit (that is, a Remote Office 9150 unit or MIG RLC) in one of two ways:

- Connect to, and then log on to the unit by serial port or Telnet (which requires Ethernet network connectivity).

  Once the connection is established, Configuration Manager displays the current configuration on the unit to which you are connected. When the configuration details appear, you can make changes and update the unit’s flash memory immediately by clicking Send, and then performing a Save to Flash.
- Perform an offline configuration (which consists of saving the configuration changes in a file on your PC), and then update a unit’s flash memory at a later time.

You can update the unit's flash memory by using one of the following methods:

- Open the configuration file within Configuration Manager, click Send, and then save it to flash.
- Initiate an upload from your PC to the unit's flash memory by using the configuration upload option in the Configuration Manager menu.

"Working with configuration files" on page 131 describes how each of these operations works.

Logging on to a unit

If you want to update a unit as you make configuration changes, or view logs and statistics, you must log on to the unit. Each unit has its own administration password.

You can log on to the unit by using one of the following connection methods:

- Telnet (over the IP network)
- serial port

For more information, see "Logging on to a unit" on page 137.

Starting Configuration Manager

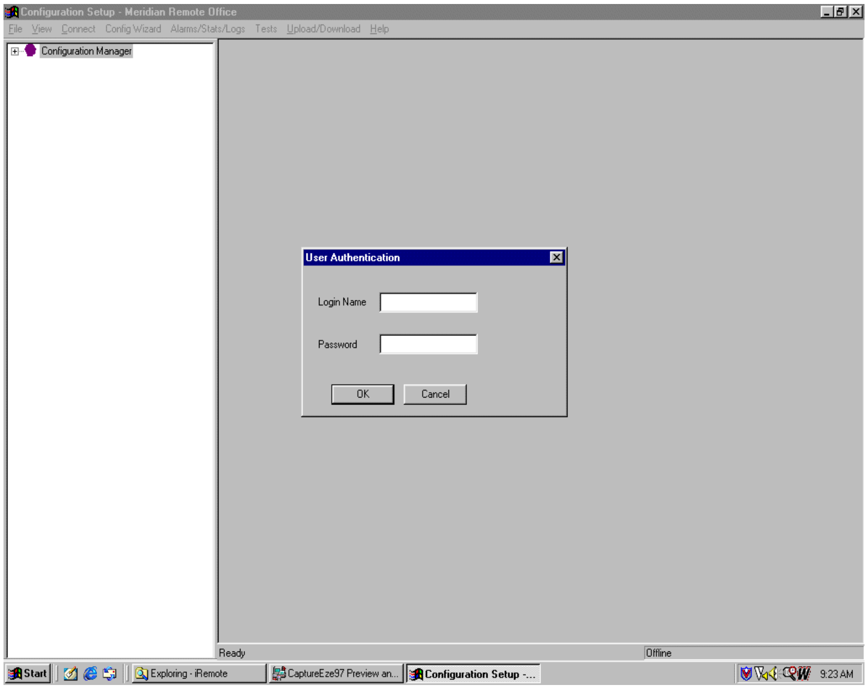
Introduction

To perform administrative tasks, you must first start the Configuration Manager software.

To start Configuration Manager

1 Click Start → Programs → Remote Office → Configuration Manager.

Result: The Configuration Manager opens and you are prompted for the logon name and password.



2 Type **admin** in the Login Name box.

3 Type **root** in the Password box.

Note: This is the default password. It might be different.

4 Click OK.

Result: You are informed if the logon was successful.

5 Click OK.

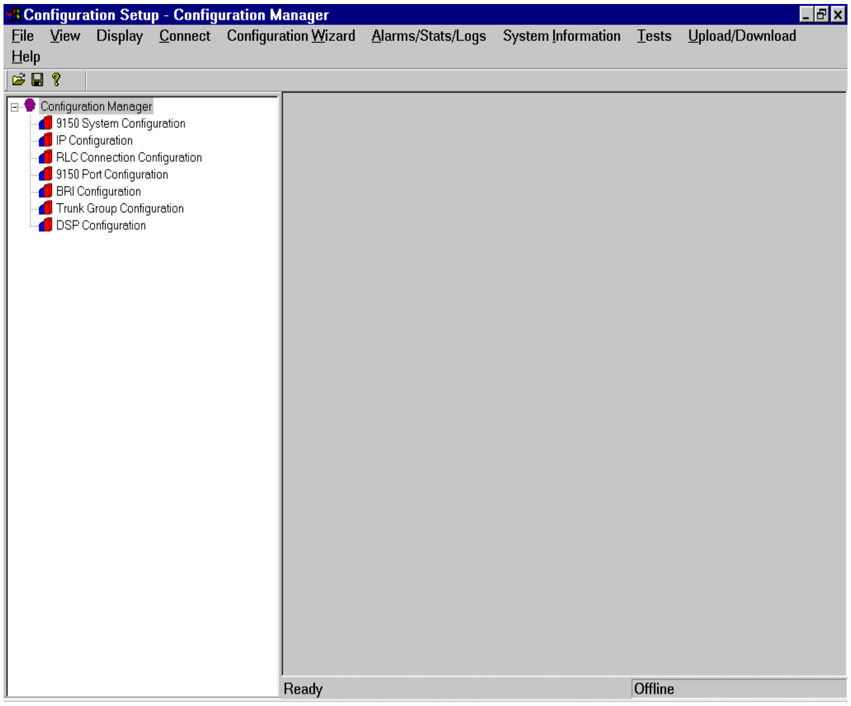
Result: The Login Name dialog box disappears.

6 Proceed as follows:

To perform an	See
online configuration	“Logging on to a unit” on page 137.
offline configuration	“Selecting the device type for offline configuration” on page 135.

7 To view the system tree, click the plus sign beside Configuration Manager in the left pane.

Result: Based on the system type you are working with, the system tree expands, showing you the types of configuration you can work with. An example is shown on page 114.


Configuration Setup - Configuration Manager
File View Display Connect Configuration Wizard Alarms/Stats/Logs System Information Tests Upload/Download Help
Configuration Manager
9150 System Configuration
IP Configuration
RLC Connection Configuration
9150 Port Configuration
BRI Configuration
Trunk Group Configuration
DSP Configuration
Ready
Offline

Configuration Manager description

Introduction

This section describes each part of the Configuration Manager screens.

Parts of the Configuration Manager screen

The Configuration Manager is divided into three parts— a menu and two panes.

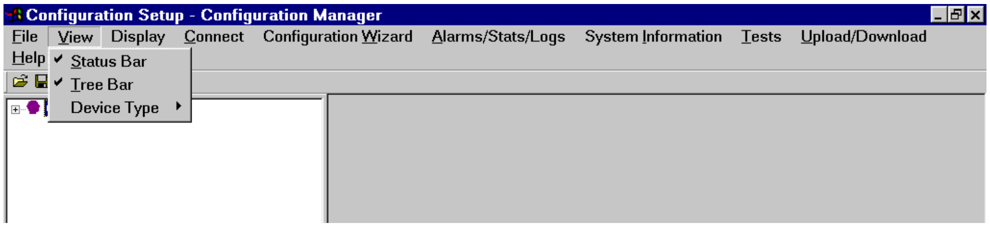
- The menu across the top of the screen lists various administrative tasks you can perform. These tasks are common to all Remote Office units.
- The pane on the left lists the property sheets you can work with. In this guide, the left pane is called the *system tree*.
- The pane on the right displays the screen associated with an item you selected from the system tree. In this guide, the right pane is called the *property sheet*.

Menu

The menu across the top of the screen provides access to system display and reporting options.

When you click an option on the menu, a drop-down list appears. When you select an option from the drop-down list, the screen associated with that option appears.

Note: Options that appear dimmed cannot be used for the unit you are working with, or if you are working offline (that is, when you are not logged on to any unit).



How this guide presents instructions for selecting menu options

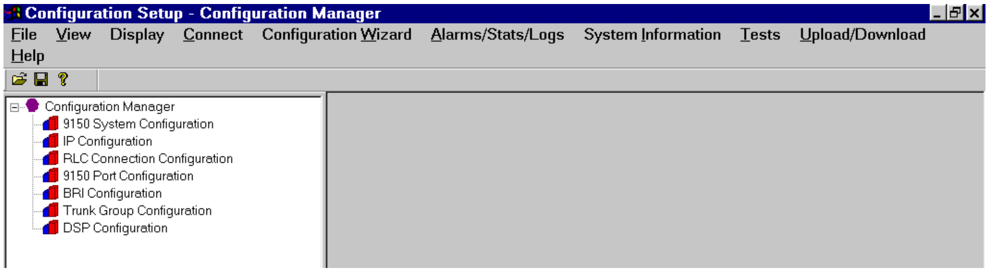
To simplify the instructions for selecting options from the menu, this guide abbreviates the selection path. For example, if a procedure requires you to choose Over IP from the Remote Connectivity menu, which is under the Tests menu, this guide uses the following style:

From the menu, choose Tests → Remote Connectivity → Over IP.

System tree

The left pane of the Configuration Manager lists property sheets you can work with. To view a list of all the property sheets associated with a system, click the plus sign to expand the list. (To hide the list, click the minus sign.)

The following example shows an expanded system tree for the Remote Office 9150 unit:



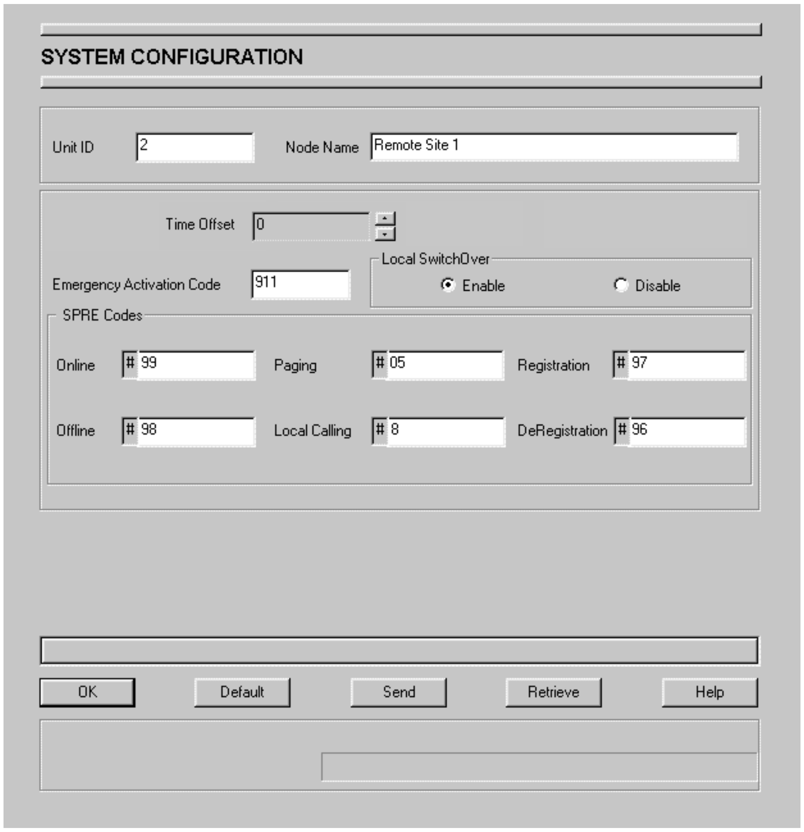
You can hide the system tree. To do this, choose View → Tree Bar. The screen redisplays, showing only the property sheet pane.

To redisplay the system tree, choose View → Tree Bar again.

Property sheets

When you are logged on to a particular system (that is, a Remote Office 9150 unit or MIG RLC), and you click an item in the system tree, the associated property sheet appears in the right pane. For instructions on selecting a device type when not logged on, see “Selecting the device type for offline configuration” on page 135.

The following is an example of the property sheet associated with the 9150 System Configuration system tree option:



SYSTEM CONFIGURATION

Unit ID 2 Node Name Remote Site 1

Time Offset 0

Emergency Activation Code 911

Local SwitchOver: ● Enable ○ Disable

SPRE Codes

Online	# 99	Paging	# 05	Registration	# 97
Offline	# 98	Local Calling	# 8	DeRegistration	# 96

How this guide presents instructions for displaying property sheets

To simplify the procedures for accessing property sheets throughout this guide, the instructions for displaying a particular property sheet are summarized into a “Getting there” statement.

The procedure for displaying the screen you need depends on whether you are

- performing an online configuration (that is, you are connected to a unit by serial port or Telnet)
- performing an offline configuration (that is, you are not connected to a unit)
- working with the system tree visible

Example

Getting there 9150 → Configuration Manager → IP Configuration

The following is the long instruction for this example:

1 Do the following:

IF you are performing an	THEN
offline configuration	select the 9150 device type as described in “Selecting the device type for offline configuration” on page 135.
online configuration	connect to, and then log on to the Remote Office 9150 unit as described in “Logging on to a unit” on page 137.

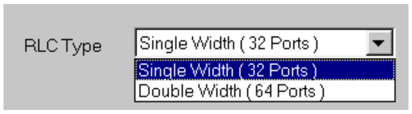
2 Navigate to the IP Configuration screen as follows:

IF the system tree is	THEN
visible	do the following: **a** Click the plus sign beside Configuration Manager to expand the system tree. **b** Click IP Configuration.
hidden	from the menu, choose Display → IP Configuration.

Result: The IP Configuration property sheet appears in the right pane.

List boxes

Boxes that provide a limited list of values are called *list boxes*. To view the values available for a list box, click the down arrow for that list box. To select an item from the list, move the cursor until the desired item is highlighted, and then click the item. The item you select appears in the list box.



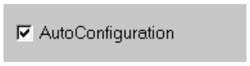
RLC Type: Single Width (32 Ports)

In some cases, selecting a particular list item causes the property sheet contents to change as follows:

- Some fields appear dimmed (disabled) because they cannot be configured in the context of the list item you selected.
- Other fields are reenabled (no longer appear dimmed).
- One or more values on the property sheet are replaced with values that are specific to the item you selected.

Check boxes

Fields that contain a blank box beside them are called *check boxes*. These check boxes are used to enable or disable the feature associated with that field. To enable the feature, click the check box. A check mark appears. When you click the check box again, the check mark disappears (thereby disabling the feature).

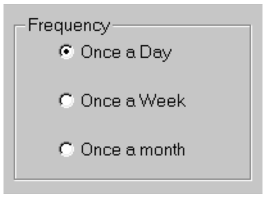


☑ AutoConfiguration

Option buttons

Some fields can have two or more options from which to select. The options contain a circle beside them, which are called *option buttons*. For these fields, only one option can be selected.

To enable an option, click the button for the option you need. If the option you selected is a change, the button for the previously selected option is cleared.



Frequency

● Once a Day

○ Once a Week

○ Once a month

In some cases, selecting a particular option button causes the property sheet contents to change as follows:

- Some fields appear dimmed (disabled) because they cannot be configured in the context of the option you selected.

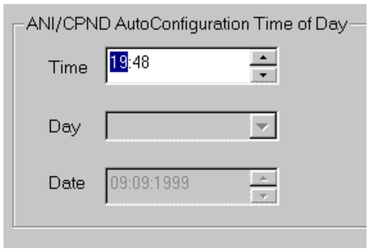
- Other fields are reenabled (no longer appear dimmed).
- One or more values on the property sheet are replaced with values that are specific to the option you selected.

Scroll boxes

Boxes that contain data with up and down arrows beside them are called *scroll boxes*. When you click the data, and then the up arrow, the selected data increases in value. When you click the down arrow, the selected data decreases in value.

You can also change the data by manually entering it. To do so, highlight the data you want to change, and then type over it.

The following screen is an example of a scroll box:



ANI/CPND AutoConfiguration Time of Day

Time: 19:48

Day:

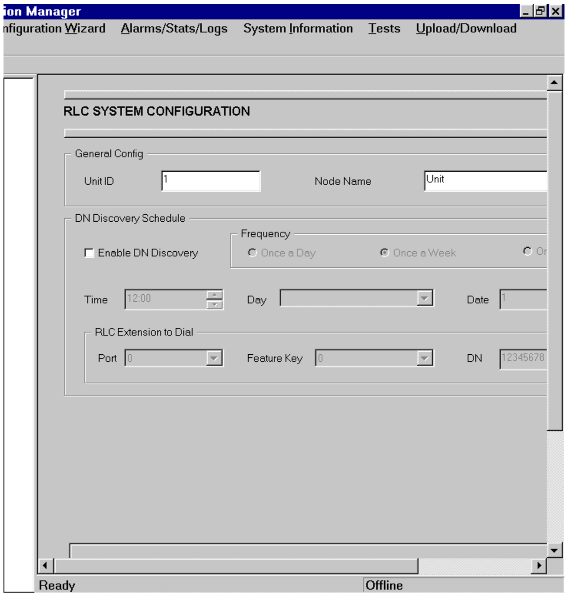
Date: 09:09:1999

Scroll bars

If your monitor’s display settings are configured so that not all the information can be displayed at once, horizontal and vertical scroll bars might appear in Configuration Manager. Some fields and buttons might be hidden. An example is shown on the next page.

The Configuration Manager software application is best viewed when your monitor settings are configured as 1024 by 768 pixels using Small Fonts at 96 dpi. This ensures that all fields and buttons are visible.

For instructions on changing your display settings, refer to the Windows online Help on your PC.



RLC SYSTEM CONFIGURATION

General Config

Unit ID 1

Node Name Unit

DN Discovery Schedule

☐ Enable DN Discovery

Frequency

○ Once a Day ● Once a Week ○ O

Time 12:00

Day

Date 1

RLC Extension to Dial

Port 0

Feature Key 0

DN 12345678

Ready

Offline

You can prevent these scroll bars from appearing by changing the screen area pixel and font sizes in the Windows Control Panel display settings on your PC.

Command buttons

The following command buttons appear on all property sheets:

- OK

  OK accepts any changes you make and stores them in a temporary file on your PC until you are ready to update the unit’s flash memory. For more details, see “OK” on page 127.

- Default

  Default replaces the values displayed on the property sheet with default values.

- Send

  Send updates to the buffer of the unit to which you are logged on with any changes you have made to the configuration. For more details, see “Send” on page 128.

- Retrieve

  Retrieve downloads the unit’s configuration from the buffer on the unit to which you are logged on and displays it in Configuration Manager on your PC. For more details, see “Retrieve” on page 128.

- Help

  Help displays online Help for the property sheet you are working with. For other methods of displaying Help, see “Using the online Help” on page 123.

Note: If the command buttons are not visible, use the vertical scroll bar to scroll through the screen.

Using the online Help

Introduction

While using the Configuration Manager, you might have questions about what certain boxes and buttons do, as well as how to complete certain tasks. Online Help provides brief answers to such questions.

To access Help

1. Use one of the following methods:
   - Method 1: Click Help on the property sheet for which you need help.
   - Method 2: From the Help menu, choose Help → Help Topics.
   - Method 3: Click ? in the toolbar.
   - Method 4: Press F1 on the keyboard.
2. If you selected methods 2, 3, or 4, go to one of the following tabs, based on how you want to search for a topic:
   - To see a list of Help topics, click the Contents tab.
   - To look up a subject alphabetically, click the Index tab.
   - To do a full-text search to find topics that contain the words you enter, click the Find tab.

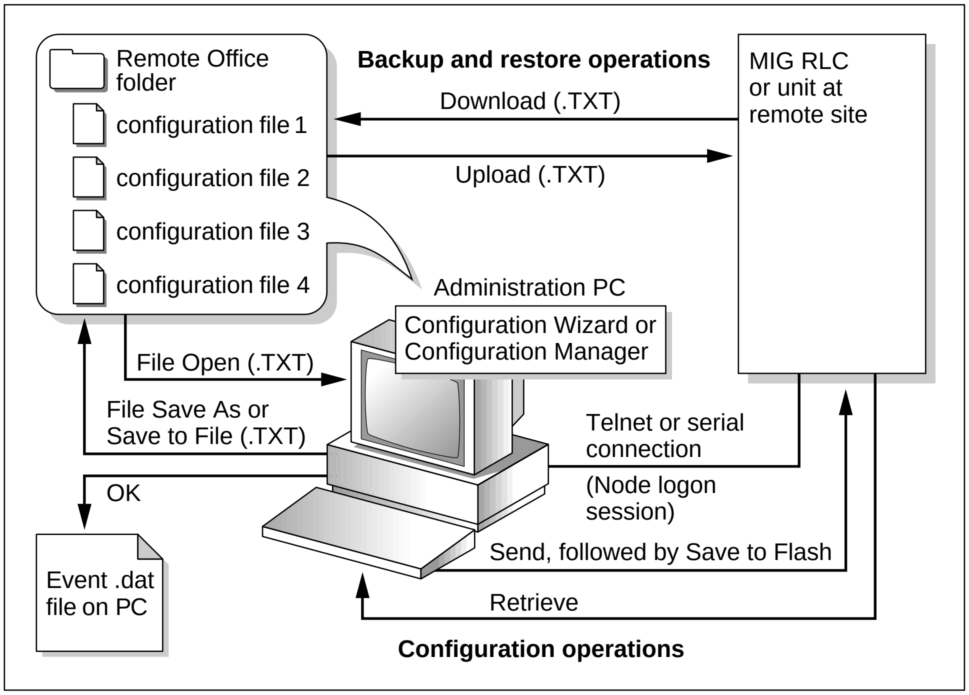
Configuration files description

Introduction

This section describes configuration files and the ways in which you can work with them.

Configuration Manager: File operations diagram

The following diagram shows how configuration information is stored. A detailed description of each file type and operation follows.



G101411

Types of files

There are four types of files that you can work with in Configuration Manager. Each file is identified by one of the following file name extensions as described in the following table:

File name	File type	When it is created and used
EVENT.DAT	Log file	This file records all activities (and messages associated with those activities) that you perform while running Configuration Manager, such as ■ logging on to Configuration Manager ■ logging on to a unit (by serial or Telnet connection) ■ logging off from the unit ■ performing configuration changes ■ performing firmware upgrades This file can be very useful when performing troubleshooting for system problems. If you need technical support, you might be asked to provide this file. **Note:** Information is appended to this file each time you start a new Configuration Manager session.
*.TXT	Text	The text file is created when you do one of the following: ■ Click Save to File while running the Configuration Wizard. ■ Click File → Save As while working in Configuration Manager. ■ Choose Upload/Download → Download Configuration to save a unit’s configuration in a text file on the administration PC.

File name	File type	When it is created and used
*.TXT (continued)	Text	To view or make changes to the text file (while in online or offline mode), do one of the following to open the file: ■ Click Open while running the Configuration Wizard. ■ Click File → Open while running Configuration Manager. ■ Choose Upload/Download → Upload Configuration to load the configuration file to the unit's buffer. For more details about these tasks, see ■ "Working with configuration files" on page 131 ■ "Performing backups and restores" on page 205. **Note:** You can view or edit the contents of the text file by opening it in a word processing application, such as WordPad.
*.UPG	Upgrade	Use this file type when performing firmware upgrades. For more details, see "Performing upgrades" on page 197.

Configuration Manager: File operations description

The following table describes each operation shown in the previous diagram:

Operation	Description
OK	When you click OK, the following occurs: ■ The changes you make are checked for errors. If errors are found, an error dialog box appears. Make the necessary changes, and then click OK again. ■ The changes you make are stored in the event.dat file on your PC. For more information about the event.dat file, see “Types of files” on page 125. To update the flash memory of the unit to which you are logged on, you must click Send, and then perform a Save to Flash. For more details, see “Send” on page 128. **Note:** If you do not click OK on a property sheet before displaying another property sheet, all changes made on the property sheet are lost and must be reentered.
File → Open	When you choose File → Open from the Configuration Manager menu, you can open a previously saved configuration file. This is useful for preparing and storing configuration files in a central location before they are deployed to the network. **Note:** To open a file, the file type must be text (.txt).
File → Save As	When you choose File → Save As from the Configuration Manager menu, the unit’s configuration is saved to a configuration file on your PC. You specify the file name and directory location. After you save the file, you can open and modify the file at another time. **Notes:** ■ The file is saved as a text (.txt) file. ■ If you close Configuration Manager without performing a File → Save As, all changes you made are lost.

Operation	Description
Send	When you click Send on a property sheet, any changes you make to this property sheet are sent to the buffer on the unit to which you are connected. If the send is successful, `Data Sent Successfully` appears. **Note:** You must perform an Upload/Download → Save to Flash to save the changes in the unit's flash memory. For more details, see Save to Flash below.
Send All	When you choose Upload/Download → Send All on any property sheet, changes for *all* property sheets are sent to the buffer on the unit to which you are connected. If the send is successful, `Data Sent Successfully` appears. **Note:** You must perform an Upload/Download → Save to Flash to save the changes in the unit's flash memory. For more details, see Save to Flash below.
Retrieve	When you click Retrieve on a property sheet, the configuration stored on the unit to which you are connected appears in Configuration Manager. If the retrieve is successful, `Data Received Successfully` appears.
Save to Flash	When you choose Upload/Download → Save to Flash, the information stored in the unit's buffer is saved to flash memory. This prevents the configuration from being lost if a power loss occurs on the unit. While in progress, `Save to Flash in Progress` appears in the status bar at the bottom of the screen. When the save to flash is completed, the Data Stored to Flash dialog box appears. **Note:** You must perform a Send or Send All before you perform a Save to Flash. You should perform a Save to Flash as often as required.

Operation	Description
Upload Configuration	When you choose Upload/Download → Upload Configuration from the Configuration Manager menu, the configuration file you specify is uploaded and written to the buffer on the unit to which you are connected. Use this option if you need to restore or replace an entire configuration. You must perform a Save to Flash from the Upload/ Download Menu to save the changes in the unit’s flash memory. If you do not perform a Save to Flash and a power loss occurs on the unit, the changes are lost. While in progress, `Save to Flash in Progress` appears in the status bar at the bottom of the screen. When the Save to Flash is completed, the Data Stored to Flash dialog box appears. **Notes:** ■ To upload a configuration file, the file type must be text (*.txt). ■ To perform a configuration upload over the IP network, a TFTP server application must be running on your PC. Uploads over the serial port are not supported. ■ The upload operation does not affect the event.dat file on the PC. ■ The new configuration does not take effect until you restart the unit. For instructions on how to restart the unit, see “Performing a system restart or shutdown” on page 146.

Operation	Description
Download Configuration	When you choose Upload/Download → Download Configuration from the Configuration Manager menu, the configuration stored on the unit to which you are connected is saved to a file on the PC. Use this option if you want to create a backup of the unit's configuration. **Notes:** ■ The downloaded file is saved as a text file (*.txt). ■ The download operation does not affect the event.dat file on the PC. Therefore, if you make changes and do not save them, they are lost.

Working with configuration files

Introduction

This section explains how to

- create a configuration file (see page 132)
- open a configuration file in Configuration Manager (see page 133)
- perform a configuration upload (see page 134)
- perform a configuration download (see page 134)

When to use the Configuration Manager file operations

You can use	When you are
OK, File → Open, and File → Save As	working in offline mode or connected and logged on to a unit. **Note:** When working in offline mode, you must save the configuration to a file. However, when you are connected and logged on to a unit, the file save operation is optional when you use Send or Send All to update the unit's flash memory.
■ Send ■ Send All ■ Retrieve ■ Upload Configuration ■ Download Configuration	connected and logged on to a unit.

To create a configuration file on the PC

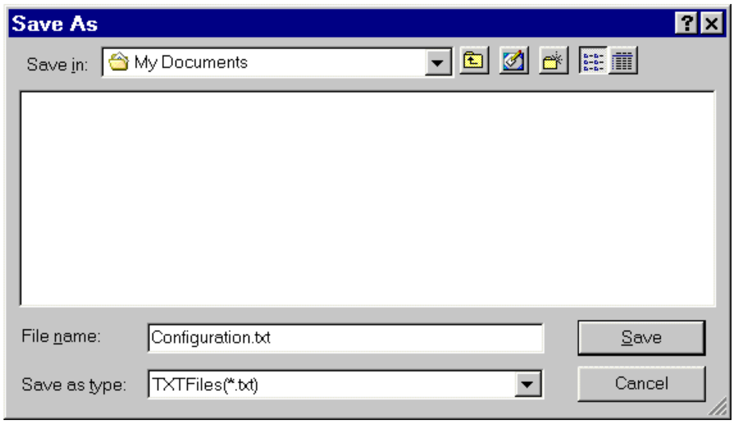
1 Start Configuration Manager.

2 Make the required changes on each property sheet.

Note: You do not have to be logged on to a unit to make configuration changes. When you are not logged on to a unit, you are performing an offline configuration.

3 From the menu, choose File → Save As.

Result: The Save As dialog box appears.



Save in: My Documents

File name: Configuration.txt

Save as type: TXTFiles(*.txt)

4 Enter a descriptive name for the file.

It should identify the type of configuration it contains.

Example 1: If the file contains basic configuration that will be used for all similar-type units, you can type **template** as the file name.

Example 2: If the file contains configuration that is unique to a specific unit, enter the unit’s name or number as the file name.

5 Ensure the Save as type box shows Text Files(*.TXT).

6 Specify the folder where the file is to be saved.

7 Click OK.

Result: The file is saved.

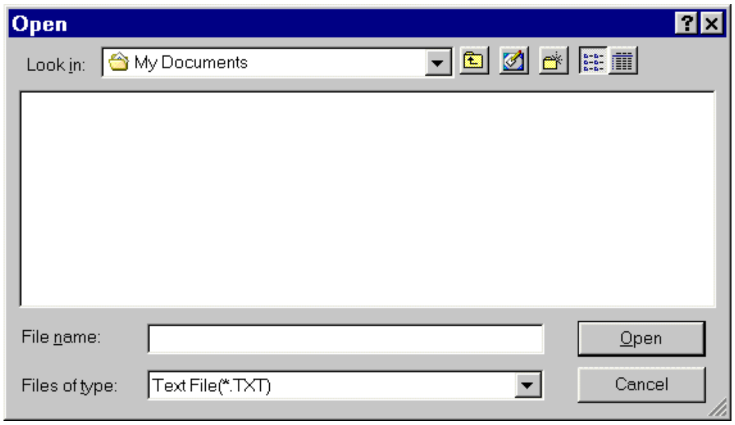
To open a configuration file

1 Start Configuration Manager.

2 If you want to work in online mode, log on to the unit. Otherwise, ensure that you have selected the device type.

3 From the menu, choose File → Open.

Result: The Open dialog box appears.



4 Ensure the Files of type box shows Text Files(*.TXT).

5 Navigate to the folder containing the file you need.

6 Select the file, and then click Open.

Result: The contents of the configuration file are loaded into Configuration Manager.

7 View the configuration details by clicking each item in the system tree to display the associated property sheet.

8 Make changes as necessary, and then do one of the following:

a. Resave the file.

b. Click Send to update the unit, and then perform a Save to Flash.

To upload a configuration to a unit

For instructions, see “Restoring the configuration” on page 209.

To download a configuration from a unit

For instructions, see “Creating a backup configuration file” on page 207.

Selecting the device type for offline configuration

Introduction

If you are not logged on to a particular system (that is, a MIG RLC or a Remote Office 9150 system), you must select the type of device with which you want to work.

When you select the device type, it causes the Configuration Manager application to automatically reorganize the system tree with the screens associated with that device type.

To select the device type

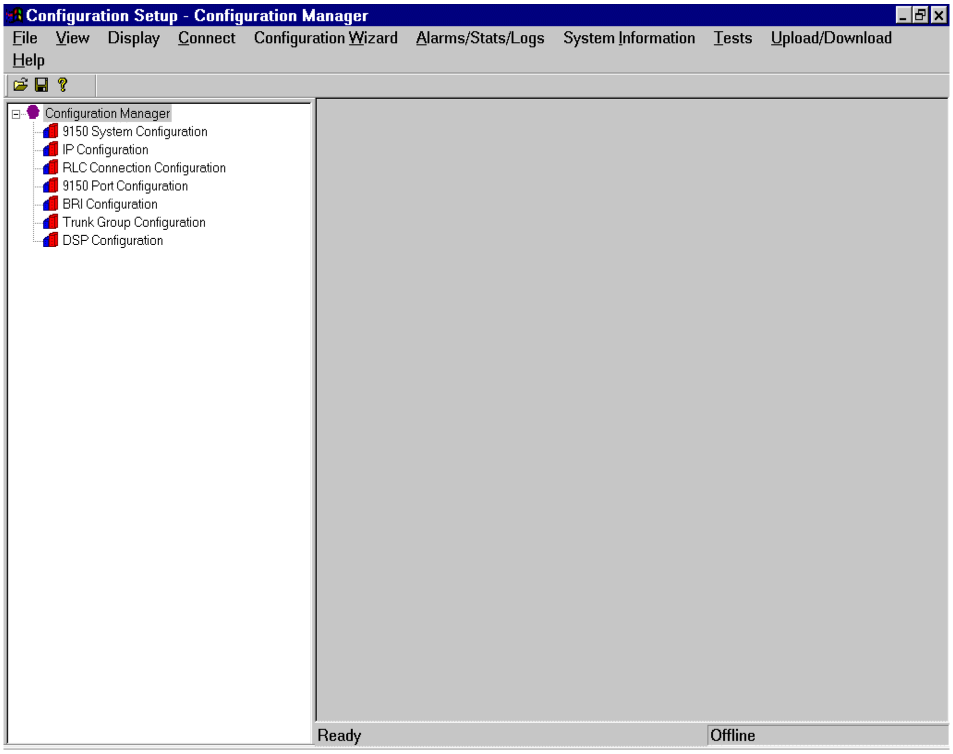
1 Start Configuration Manager as described in “Starting Configuration Manager” on page 112.

2 Do the following:

To view the system tree for	**Do the following**
the MIG RLC	Choose View → Device Type → RLC.
the Remote Office 9150 unit	Choose View → Device Type → 9150.

3 Click the plus sign beside Configuration Manager in the left pane.

Result: The system tree expands, showing you the types of configuration you can work with, as shown in the example on page 136.



Configuration Setup - Configuration Manager
File View Display Connect Configuration Wizard Alarms/Stats/Logs System Information Tests Upload/Download Help
Configuration Manager
9150 System Configuration
IP Configuration
RLC Connection Configuration
9150 Port Configuration
BRI Configuration
Trunk Group Configuration
DSP Configuration
Ready
Offline

Logging on to a unit

Introduction

If you want to update the flash memory on a unit as you make configuration changes, or view statistics and logs, you must log on to the unit. Each unit has its own administration ID and password.

You can log on to the unit by using one of the following connection methods:

- Telnet (over the IP network)
- serial port

Connection types

If the MIG RLC or Remote Office 9150 unit is connected to the administration PC by the RS-232 cable, you can establish a connection through the serial port.

If Ethernet connectivity has been established between the administration PC and the MIG RLC or Remote Office 9150 unit, you can establish an IP connection with Telnet.

Connection history

The Configuration Manager maintains a history of past unit connections. You can select and then connect to a unit from the history list that appears in the Connect menu.

Note: The connection history list is deleted each time you upgrade the Configuration Manager software.

Default logon ID and password

The default logon ID is **guest**. It cannot be changed.

The default password is **guest123**. The password can be different if it was changed.

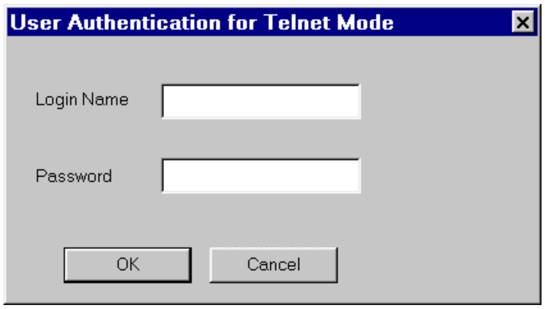
Auto logoff

If the connection has remained active with no activity for 15 minutes or more, you are automatically logged off and the Session Timed Out message appears. This helps to secure the configuration in the event that you walk away from the administration PC while logged on to a unit.

To log on to a unit using the connection history

1 From the menu, choose Connect → IP address of the unit to which you want to log on.

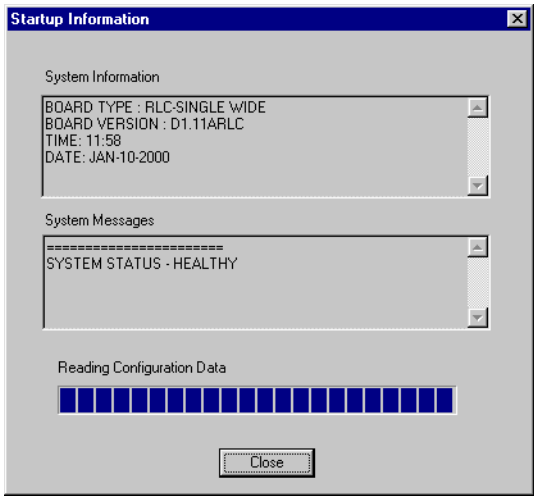
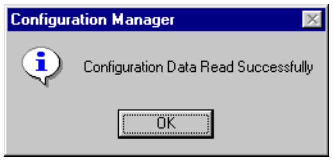
Result: The User Authentication for Telnet Mode dialog box appears.



2 Enter your logon name and password, and then click OK.

Result: The connection attempt is initiated. `Trying to Connect to <IP address>` message might appear.

IF the logon attempt	THEN
failed	the following message appears: `10060 TELNET CONNECTION FAILED` Go back to step 1.

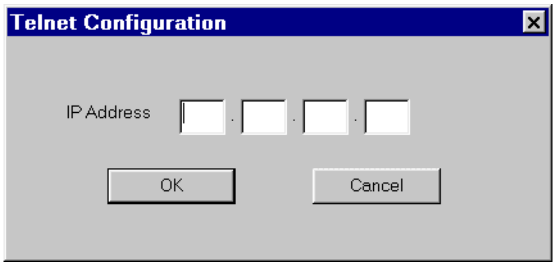
IF the logon attempt	THEN
succeeded	the User Logged In dialog box appears. Click OK. **Result:** The following dialog box appears:  Startup Information System Information BOARD TYPE : RLC-SINGLE WIDE BOARD VERSION : D1.11ARLC TIME: 11:58 DATE: JAN-10-2000 System Messages ====================== SYSTEM STATUS - HEALTHY Reading Configuration Data The following messages appear above the progress bar at the bottom of the dialog box: ■ Reading Hardware Information ■ Reading DSP Load Data ■ Reading Configuration Data These messages mean that Configuration Manager is obtaining the unit's configuration information from flash memory. When initialization completes, the following dialog box appears:  Configuration Manager Configuration Data Read Successfully Click OK.

To log on to a unit using Telnet

Note: If someone else is already logged on to the unit, you cannot log on.

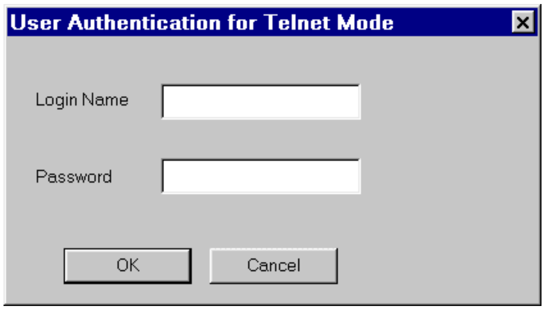
1 From the menu, choose Connect → Login board → Telnet.

Result: The Telnet Configuration dialog box appears.



2 Enter the IP Address of the unit to which you want to connect, and click OK.

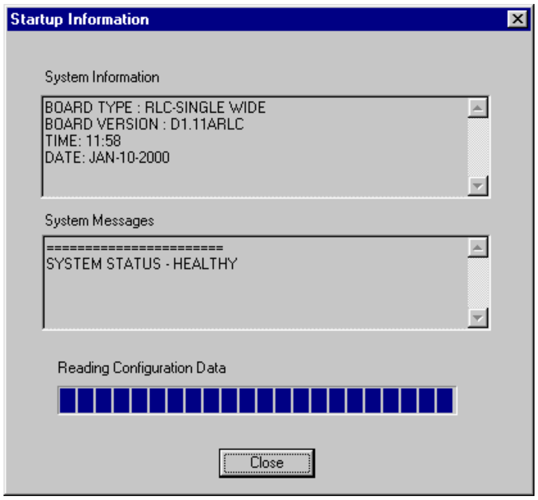
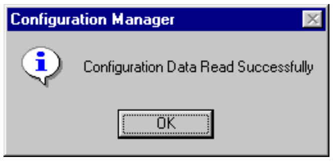
Result: The User Authentication for Telnet Mode dialog box appears.



3 Enter your logon name and password, and then click OK.

Result: The connection attempt is initiated. The message `Trying to Connect to <IP address>` message might appear.

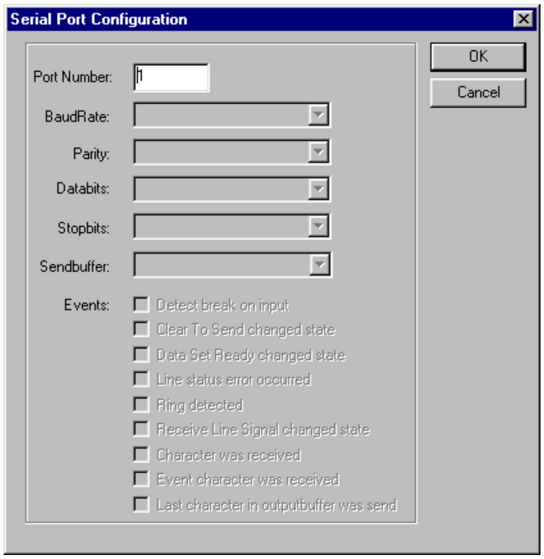
IF the logon attempt	THEN
failed	the following message appears: `10060 TELNET CONNECTION FAILED` Go back to step 1.

IF the logon attempt	THEN
succeeded	the User Logged In dialog box appears. Click OK. **Result:** The following dialog box appears:  BOARD TYPE : RLC-SINGLE WIDE BOARD VERSION : D1.11ARLC TIME: 11:58 DATE: JAN-10-2000 ======================= SYSTEM STATUS - HEALTHY Reading Configuration Data The following messages appear above the progress bar at the bottom of the dialog box: ■ Reading Hardware Information ■ Reading DSP Load Data ■ Reading Configuration Data These messages mean that Configuration Manager is obtaining the unit's configuration information from flash memory. When initialization completes, the following dialog appears:  Configuration Data Read Successfully Click OK.

To log on to a unit using the serial port

1 From the menu, choose Connect → Login board → Serial.

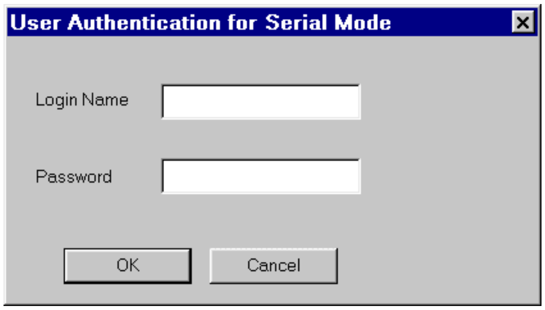
Result: The Serial Port Configuration dialog box appears.


Serial Port Configuration
OK
Cancel
BaudRate:
Parity:
Databits:
Stopbits:
Sendbuffer:
Events:
□ Detect break on input
□ Clear To Send changed state
□ Data Set Ready changed state
□ Line status error occurred
□ Ring detected
□ Receive Line Signal changed state
□ Character was received
□ Event character was received
□ Last character in outputbuffer was send

Port Number: 1

2 Enter the COM port number to which the unit is connected, and then click OK.

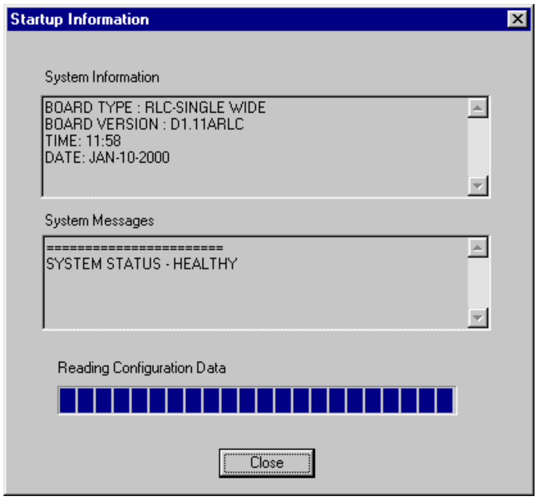
Result: The User Authentication for Serial Mode dialog box appears.



3 Enter your logon name and password, and then click OK.

Result: The connection attempt is initiated. The message `Trying to Connect via Serial Port <port number>` might appear.

IF the logon attempt	THEN
failed	the following message appears: `SERIAL CONNECTION FAILED` Go back to step 1.
succeeded	the User Logged In dialog box appears. Click OK. **Result:** The following dialog box appears:



```
BOARD TYPE : RLC-SINGLE WIDE
BOARD VERSION : D1.11ARLC
TIME: 11:58
DATE: JAN-10-2000
```

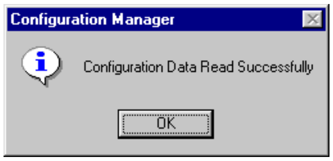
```
=======================
SYSTEM STATUS - HEALTHY
```

Reading Configuration Data

The following messages appear above the progress bar at the bottom of the dialog box:

- Reading Hardware Information
- Reading DSP Load Data
- Reading Configuration Data

These messages mean that Configuration Manager is obtaining the unit's configuration information from flash memory.

IF the logon attempt	THEN
succeeded (continued)	When initialization is completed, the following dialog box appears:  Configuration Data Read Successfully Click OK.

To access property sheets associated with the unit

1 Click the plus sign beside Configuration Manager.

Result: This expands the system tree.

2 Click the name of the property sheet with which you want to work.

Result: The property sheet appears in the right pane.

Logging off from a unit

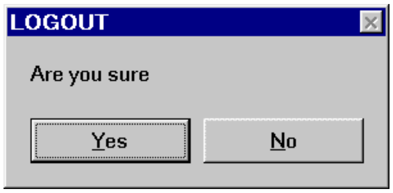
Introduction

When you are finished using Configuration Manager to make configuration changes, or to view logs and statistics, you should log off from the unit. Logging off secures the unit’s configuration.

To log off from the unit

1 From the menu, choose Connect → Logout Board.

Result: The LOGOUT dialog box appears.

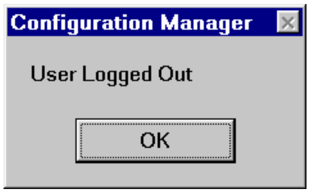


LOGOUT

Are you sure

2 Click Yes.

Result: The following dialog box appears:



Configuration Manager

User Logged Out

3 Click OK.

Performing a system restart or shutdown

Introduction

Configuration Manager allows you to perform a controlled system restart or shutdown.

When to perform a restart

You must perform a system restart each time you change the configuration or upgrade the firmware.

When to perform a shutdown

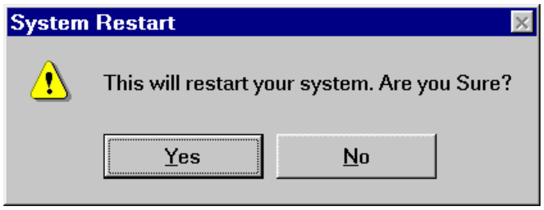
You must perform a system shutdown when

- you want to install DSP application or trunk interface modules
- you need to power down the system for any reason

To perform a system restart

1 From the menu, choose Connect → System Reset → Restart.

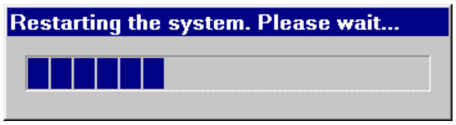
Result: The System Restart dialog box appears.



This will restart your system. Are you Sure?

2 Click Yes.

Result: The following status dialog box appears:

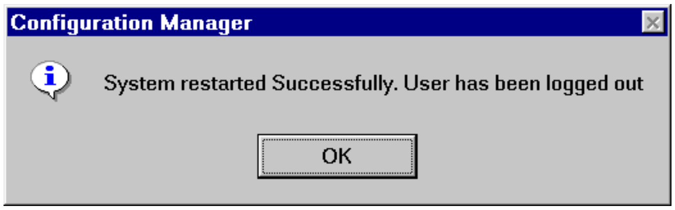


Restarting the system. Please wait...

The following message also appears in the status bar at the bottom of the screen:

```
Restarting the System
```

The status continues to show Online. When the system restart is completed, the following dialog box appears to inform you that the system restart was successful and that you were logged off:



System restarted Successfully. User has been logged out

3 Click OK.

Result: You are prompted to log back on using the previous connection method (Serial or Telnet).

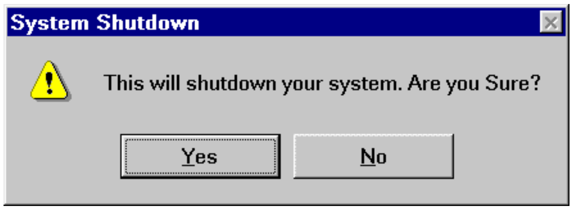
To perform a system shutdown

ATTENTION

Do not perform this procedure if you do not have physical access to the unit. To recover from the system shutdown, you must power the unit off, and then power it back on.

1 Choose Connect → System Reset → Shutdown.

Result: The System Shutdown dialog box appears.



System Shutdown

This will shutdown your system. Are you Sure?

2 Click Yes.

Result: Your logon session is disconnected, and the following message appears in the status bar at the bottom of the screen:

```
Shutting Down the System
```

The status shows Offline.

3 Turn the power off.

Note: You must turn the power off before you can power the unit back up.

Closing Configuration Manager

Introduction

When you have completed all the configuration modifications you want to make, or are done viewing unit logs and statistics, close the Configuration Manager application. This secures the configuration, preventing others from accessing it if you walk away from the administration PC while logged on to a unit.

To close Configuration Manager

CAUTION

Risk of configuration loss

If you close Configuration Manager without saving the changes you made to a file on your PC, or without updating the flash memory of the unit you were working on, all changes are lost. You must reenter any changes you made.

1 Ensure that you have saved all configuration changes by doing one or more of the following:

- From the menu, choose File → Save As, and then specify the name for the configuration file. The file is saved on the administration PC hard disk.
- Update the flash memory of the unit to which you are connected by doing one of the following:
  - Click Send or Send All on any property sheet, and then choose Upload/Download → Save to Flash.
  - If you have saved the changes to a file, choose Upload/Download → Upload Configuration.
    For instructions, see "Restoring the configuration" on page 209.

2 Log off by choosing Connect → Logout Board.

3 From the menu, choose File → Exit.

Result: The Configuration Manager closes.

Chapter 6

Configuring the Meridian Internet Gateway Reach Line Card

In this chapter

Overview

Introduction

This chapter explains how to configure the Meridian Internet Gateway Reach Line Card (MIG RLC) so that it can communicate with the remote units to which it is connected.

IP addresses

To operate as a node on the IP network, the MIG RLC needs network connectivity to

- the remote site
- an administration terminal
- the host PBX

This requires that you establish an IP address for the MIG RLC. A detailed discussion of IP addresses begins on page 153.

Remote site connections

This section discusses the configurations that are necessary to take full advantage of your Remote Office system.

Online/offline table

The online/offline table allows you to schedule the times at which an ISDN connection is available to a remote site. The online/offline table gives you the ability to ensure that the potentially expensive ISDN connection is disabled after business hours.

Section A: IP addresses

In this section

About IP addresses

Introduction

To operate as a node on the IP network, the following elements must be configured on the MIG RLC:

- an IP address
- a subnet mask
- the default gateway

These items provide network connectivity between the MIG RLC, an administration terminal, and the remote site. This connectivity allows the following events to take place:

- Voice traffic is routed between the MIG RLC and the remote site over IP.
- An administrator can use a PC located anywhere on the network to connect with any MIG RLC or remote unit on the network.

  Once connected, you can view or work with the system configuration.

  Note: To do this, the Configuration Manager software must be installed on that PC.

In addition to the IP address, subnet mask, and default gateway mentioned above, you can also assign an IP address to the management port on the MIG RLC. Once you have assigned this IP address, you can use the PBX administration PC to log on to and administer the MIG RLC via the Meridian 1 PBX’s internal network.

IP address

An IP address is a 32-bit address assigned to every host that wants to use TCP/IP to communicate across your corporate network. The address consists of a network and a host field. IP addresses are written in decimal-dot notation (for example, 123.45.67.89).

The IP address assigned to the MIG RLC must be unique, and it should conform to the addressing scheme used on your network.

Subnet mask

A network can be broken down into one or more physical networks, each of which forms a subset of the main network. This process is called subnetting or creating a subnet.

Subnets represent a way of using part of the host address to represent a smaller network. Their use provides much more flexibility when allocating IP addresses, and ensures that network traffic is not sent to the whole network unintentionally.

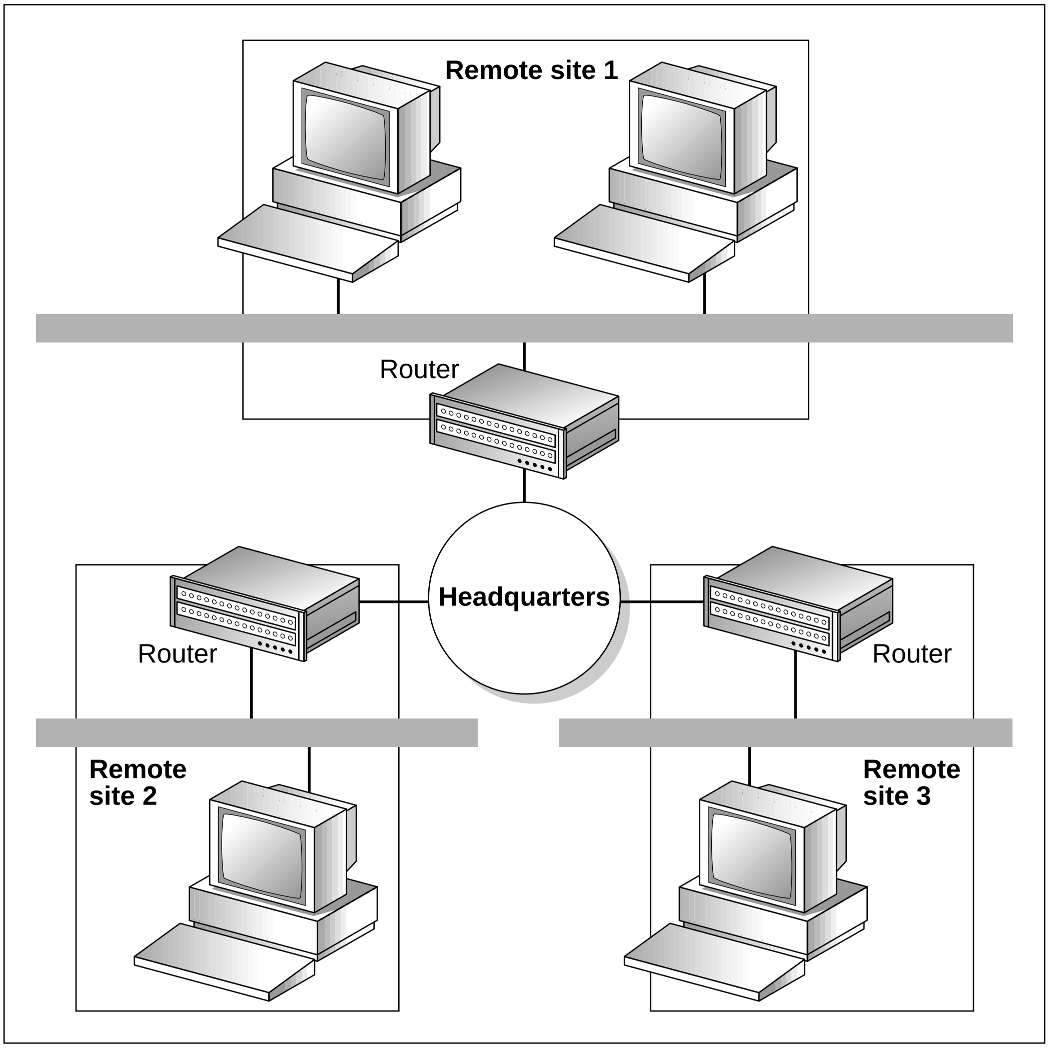
What is a subnet mask?

A subnet mask is the part of the IP address used to represent a subnetwork within a network. A typical IP address might be 192.210.34.144. Each part of this address is made up of eight bits. The subnet mask identifies to the MIG RLC what portion of the IP address represents the network (and subnetwork), and what portion represents the host.

Note: Subnet masks are a complicated feature. This section provides an overview of how they work. You should not have to alter the subnets that have been allocated in your network.

Example of subnet use

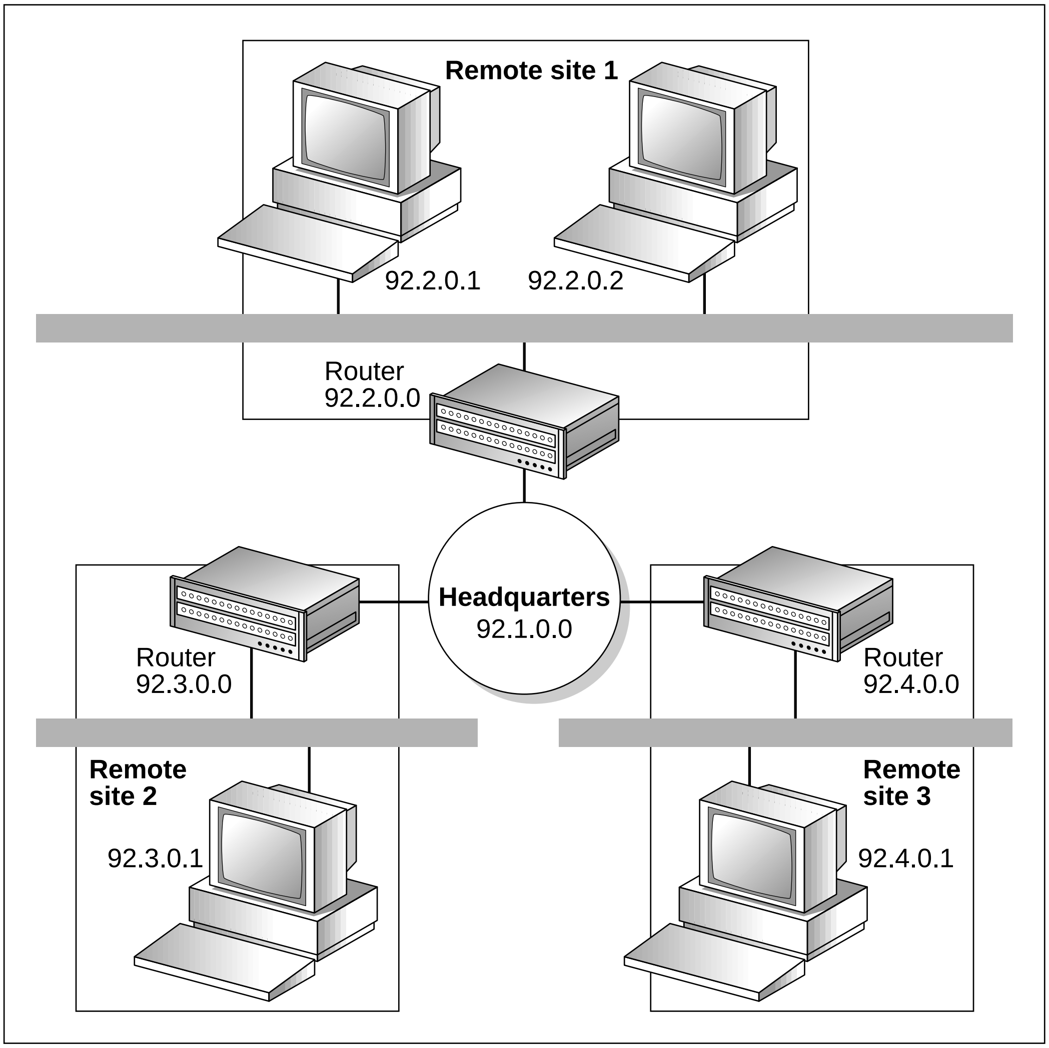
The following illustration shows a typical setup for an organization with headquarters and branch offices.



G101483

If all of the offices connect to the same network, then all of the traffic is usually sent to all of the devices all of the time. This wastes bandwidth, and it is very expensive. It is possible to use a different network for each office, but this is also expensive.

Subnets offer a solution to this problem. In the following illustration, each branch is on network 92 and has a unique subnet. Generally, traffic does not leave its subnet unless the traffic's destination is on a different subnet.



G101419

In this case, the subnet mask is 255.255.0.0. If assigned to the MIG RLC, this tells the MIG RLC that the first 16 bits of the IP address represent the network and subnetwork.

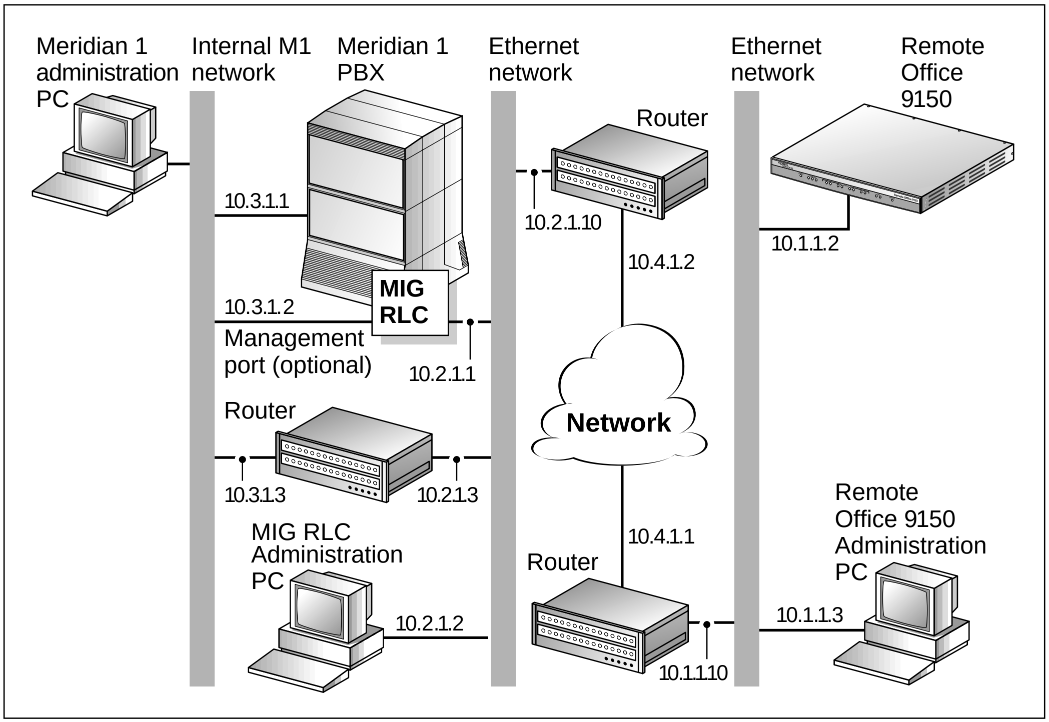
Default gateway

A gateway is a device that functions as a node on two or more networks, forwarding packets from one network to addresses in other networks.

In a MIG RLC context, the gateway is the device on the network that directs traffic to and from the MIG RLC.

Meridian Internet Gateway Reach Line Card position in your IP network

As discussed earlier in this guide, the MIG RLC is connected to a hub on your IP network. The following diagram provides an example of what the setup and the IP configuration look like:



G101400

Configuring the Reach Line Card’s IP interface

Introduction

This section explains how to enter

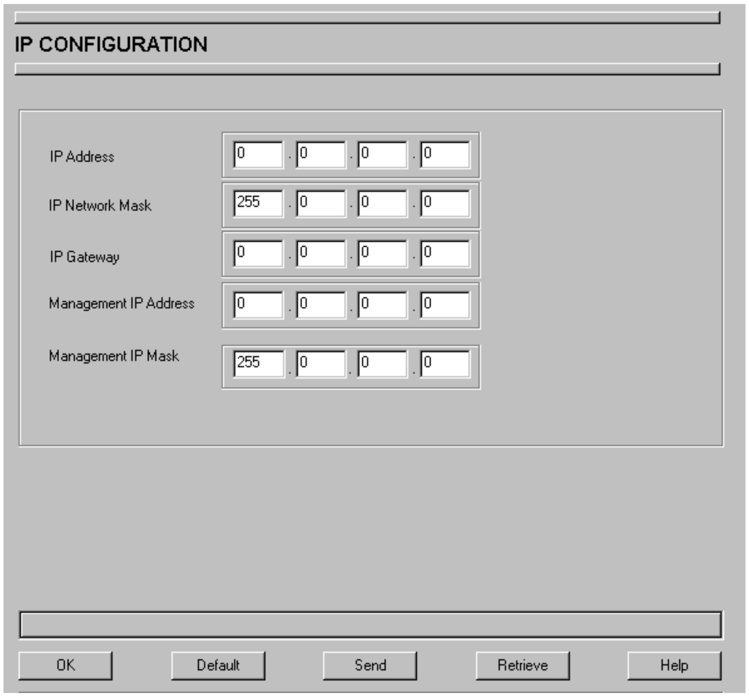
- the IP address, subnet mask, and default gateway for the primary MIG RLC Ethernet port
- the IP address for the Management MIG RLC Ethernet port used for PBX maintenance over Ethernet

For a description of each of these items, see “About IP addresses” on page 154.

Getting there

RLC → Configuration Manager → IP Configuration

IP Configuration property sheet



IP CONFIGURATION

IP Address 0 . 0 . 0 . 0

IP Network Mask 255 . 0 . 0 . 0

IP Gateway 0 . 0 . 0 . 0

Management IP Address 0 . 0 . 0 . 0

Management IP Mask 255 . 0 . 0 . 0

To enter the IP addresses

1 Type the MIG RLC's IP address into the IP Address boxes.

Press Tab to move from box to box. Press Tab again to move to the IP Network Mask row.

2 Enter the subnet mask in the IP Network Mask boxes in the same manner used in the previous step.

3 Enter the gateway's IP address in the IP Gateway boxes.

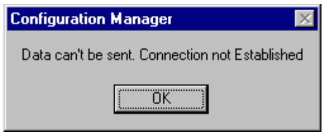
4 Enter the IP address of the MIG RLC's second Ethernet port in the Management IP Address boxes.

Note: The second Ethernet port of the MIG RLC is only available with the RLC Multi-I/O cable–Enhanced.

5 Enter the subnet mask of the MIG RLC's second Ethernet port in the Management IP Mask boxes.

6 Click OK.

7 To update the MIG RLC with the new information, click Send.

IF you are	THEN
logged on to the MIG RLC	the changes are written to a temporary file on the administration PC. **Note:** To save changes to the MIG RLC's flash memory, perform an Upload → Save to Flash.
not logged on to the MIG RLC	the following dialog box appears:  Configuration Manager Data can't be sent. Connection not Established Log on to the MIG RLC, and then click Send again.

Section B: Remote site connections

In this section

Overview

Introduction

This section discusses the configurations that are necessary to take full advantage of your Remote Office system.

RLC system configuration

There are two categories on the RLC system configuration property sheet:

- general configuration: Identify this MIG RLC within your remote network.
- DN discovery schedule: Set the times at which the MIG RLC automatically discovers the name and number assigned to the first line key for each MIG RLC remote port.

A detailed discussion of this property sheet begins on page 164.

RLC port configuration

You can configure ports on the MIG RLC as one of the following:

- remote ports, to provide host-site PBX access to a remote user station
- network ports, to establish PSTN connections between the MIG RLC and its remote units
- local ports, to provide local digital telephone connections directly to the MIG RLC, thus emulating an XDLC

A detailed discussion of the property sheet begins on page 168.

Remote connection configuration

Settings on the Remote Connection Configuration property sheet define the MIG RLC’s connection to the remote site. A detailed discussion of this property sheet begins on page 174.

Quality of Service transitioning technology

When voice quality on the IP network falls below the specified threshold and duration values, calls are moved from the IP network to the circuit-switched network. When voice quality on the IP network returns to the recover threshold and duration values, calls are moved back to the IP network.

A detailed discussion of the Quality of service dialog box begins on page 183.

RLC system configuration

Introduction

There are two categories on the RLC system configuration property sheet:

- general configuration: Identify this MIG RLC within your remote network.
- DN discovery schedule: Set the times at which the MIG RLC automatically discovers the name and number assigned to the first line key for each MIG RLC remote port.

Unit ID

The Unit ID uniquely identifies the MIG RLC from all units connected to it.

Note: You can assign a unique ID to each unit in the network; however, this is not recommended. The valid range of unit IDs is 1–255, which limits the size of your network.

DN Discovery

Through DN Discovery, the MIG RLC detects the PBX-configured name and number assigned to every line key in its portion of the remote network.

Select the criteria for DN Discovery with the fields in the “DN Discovery Schedule” section of the RLC System Configuration property sheet. For an explanation of these fields, see “RLC System Configuration field descriptions” on page 166.

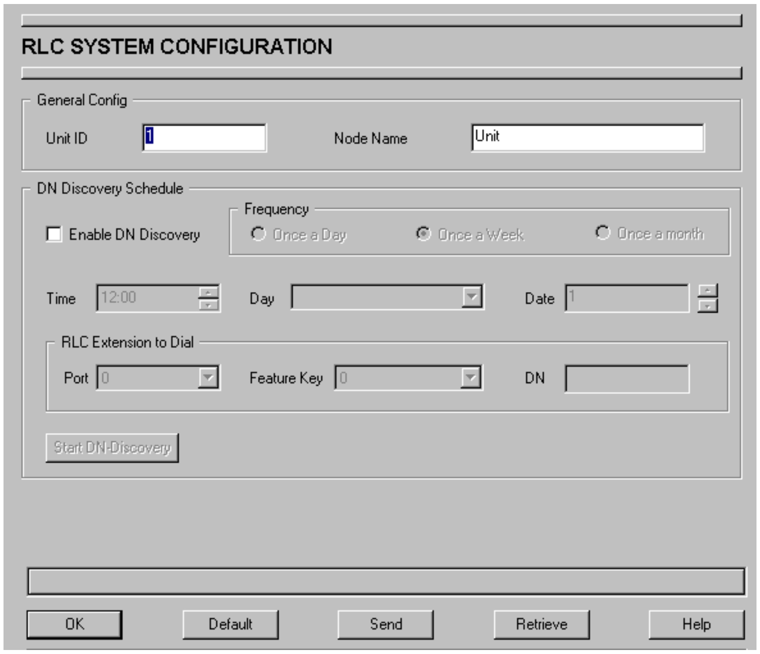
How it works

At the configured time and day, or date, the MIG RLC places a call from the first of its ports configured as Remote on the RLC Port Configuration property sheet to the DN in the RLC extension to dial: DN field on the RLC System Configuration property sheet.

The PBX regularly provides updated keymaps of the remote station’s feature keys to the MIG RLC. For each feature key configured as a line key, the MIG RLC places a call. For each call, the PBX produces CLID information, which reveals the primary DN of the remote port to which the call is placed.

Getting there RLC → Configuration Manager → RLC System Configuration

RLC System Configuration property sheet



RLC SYSTEM CONFIGURATION

General Config

Unit ID: 1

Node Name: Unit

DN Discovery Schedule

□ Enable DN Discovery

Frequency: ○ Once a Day ● Once a Week ○ Once a month

Time: 12:00

Day:

Date: 1

RLC Extension to Dial

Port: 0

Feature Key: 0

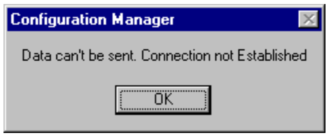
DN:

To configure the RLC system information

1 Complete the fields as described in “RLC System Configuration field descriptions” on page 166.

2 Click OK to save your settings to a temporary work file.

3 To update the MIG RLC with the new information, click Send.

IF you are	THEN
logged on to the MIG RLC	the changes are written into the MIG RLC's buffer. To save the pages in the MIG RLC's Flash memory, complete an Upload/Download → Save to Flash.
not logged on to the MIG RLC	the following dialog box appears:  Configuration Manager Data can't be sent. Connection not Established Do one of the following: ■ Log on to the MIG RLC, and then click Send again. ■ Save the changes to a file on your administration PC.

RLC System Configuration field descriptions

Field	Description
Unit ID	Enter a number between 1–255 that distinguishes this MIG RLC from all Remote Office 9150 units connected to that MIG RLC. **Note:** This Unit ID must be entered on the RLC Connection Configuration property sheet on the remote unit to create the communication path between this MIG RLC and the remote unit.
Node Name	Enter a descriptive name for this MIG RLC.

Field	Description
Enable DN Discovery	■ Select Enable if you want the MIG RLC to autodetect the PBX-configured name and number assigned to each line key for each remote port on the MIG RLC. ■ Select Disable if you do not want the MIG RLC to perform DN Discovery.
Frequency	Select the option button that identifies how often DN discovery should be performed: ■ once a day ■ once a week ■ once a month
Time	Specify the time when DN discovery should be performed.
Day	Select the day when DN discovery should be performed (if you selected “Once a week” in the Frequency field).
Date	Specify the date when DN discovery should be performed (if you selected “Once a month” in the Frequency field).
RLC extension to dial	These fields allow you to configure one MIG RLC port whose port number, feature key position, and DN are known. At the DN discovery time, each remote port on the MIG RLC will place a call to the DN in the RLC extension to dial field and the incoming CLID name and number will be assigned to the calling port for use by the remote unit: ■ Port: this list box determines to which remote site the succeeding settings in this section apply ■ Feature Key: this list box sets the feature key that initiates DN discovery at this remote site ■ DN: this field displays the directory number to dial to access the Remote Office 9150 unit at this remote site

RLC port configuration

Introduction

You can configure ports on the MIG RLC can be configured as one of the following:

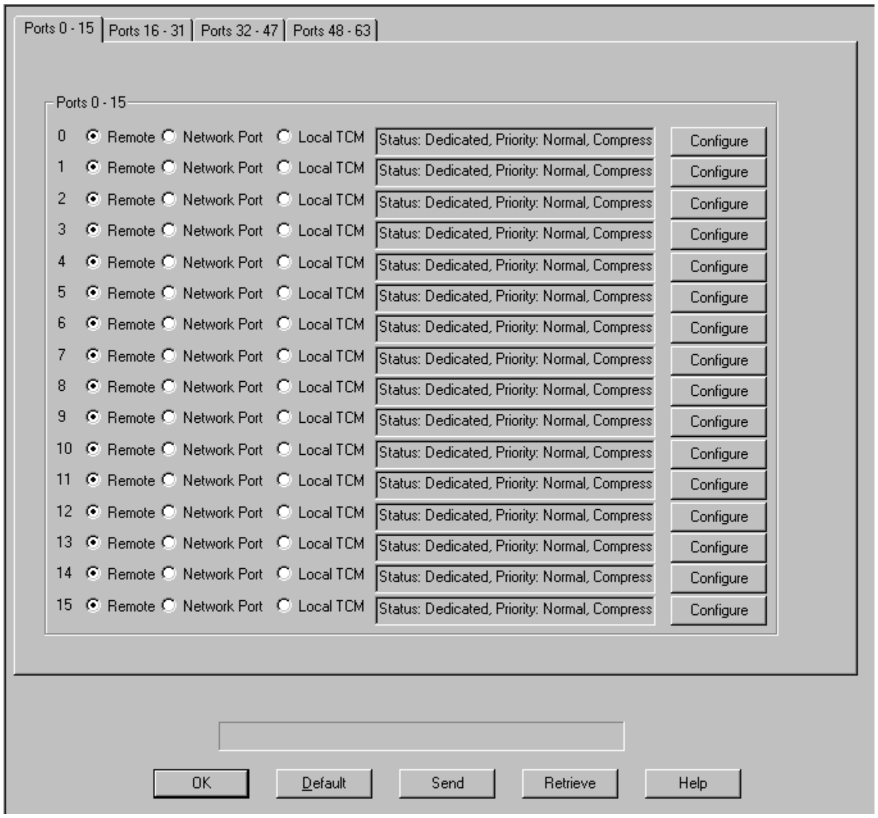
- remote ports, to provide host-site PBX access to a remote user station
- network ports, to establish PSTN connections between the MIG RLC and its remote units
- local ports, to provide local digital telephone connections directly to the MIG RLC thus emulating an XDLC

The following table describes port number ranges and how they can be configured:

Ports	Can be assigned to
0–15 and 32–47	digital telephone sets that are assigned to remote users. **Note:** The associated ports on the host PBX must be configured with voice capability.
16–31 and 48–63	■ stations equipped with ATAs or MCAs ■ network ports for configuring a trunk between the MIG RLC and a Remote Office 9150 unit **Note:** The associated ports on the host PBX must be configured with data capability.
64	a fax machine or other analog device (without an ATA). **Note:** The associated port on the host PBX must be configured with data capability.

Getting there RLC → Configuration Manager → RLC Port Configuration

RLC Port Configuration property sheet



Ports 0 - 15

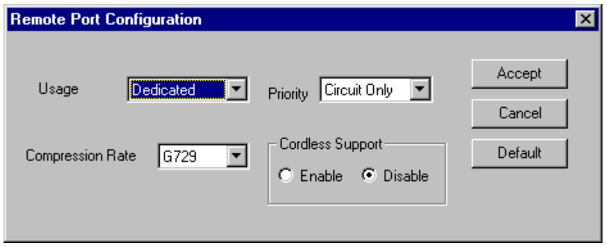
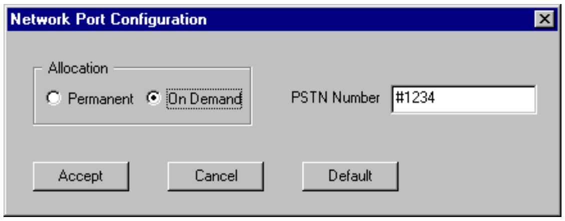
0	● Remote	○ Network Port	○ Local TCM	Status: Dedicated, Priority: Normal, Compress	Configure
1	● Remote	○ Network Port	○ Local TCM	Status: Dedicated, Priority: Normal, Compress	Configure
2	● Remote	○ Network Port	○ Local TCM	Status: Dedicated, Priority: Normal, Compress	Configure
3	● Remote	○ Network Port	○ Local TCM	Status: Dedicated, Priority: Normal, Compress	Configure
4	● Remote	○ Network Port	○ Local TCM	Status: Dedicated, Priority: Normal, Compress	Configure
5	● Remote	○ Network Port	○ Local TCM	Status: Dedicated, Priority: Normal, Compress	Configure
6	● Remote	○ Network Port	○ Local TCM	Status: Dedicated, Priority: Normal, Compress	Configure
7	● Remote	○ Network Port	○ Local TCM	Status: Dedicated, Priority: Normal, Compress	Configure
8	● Remote	○ Network Port	○ Local TCM	Status: Dedicated, Priority: Normal, Compress	Configure
9	● Remote	○ Network Port	○ Local TCM	Status: Dedicated, Priority: Normal, Compress	Configure
10	● Remote	○ Network Port	○ Local TCM	Status: Dedicated, Priority: Normal, Compress	Configure
11	● Remote	○ Network Port	○ Local TCM	Status: Dedicated, Priority: Normal, Compress	Configure
12	● Remote	○ Network Port	○ Local TCM	Status: Dedicated, Priority: Normal, Compress	Configure
13	● Remote	○ Network Port	○ Local TCM	Status: Dedicated, Priority: Normal, Compress	Configure
14	● Remote	○ Network Port	○ Local TCM	Status: Dedicated, Priority: Normal, Compress	Configure
15	● Remote	○ Network Port	○ Local TCM	Status: Dedicated, Priority: Normal, Compress	Configure

To configure a MIG RLC port

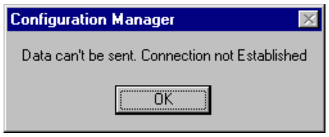
1 Click the appropriate tab for the port you are configuring:

- 0–15 or 16–31 for a single-wide MIG RLC
- 0–15, 16–31, 32–47, or 48–63 for a double-wide MIG RLC

2 In the line for the port you are configuring, choose the type of port you want to configure according to the following table:

IF you want to configure a	**THEN**
remote port	do the following: **1** Choose the remote option button on the line of the port number you are configuring. **2** Click the configure button on the same line. **Result:** The Remote Port Configuration dialog box.  Remote Port Configuration Usage: Dedicated Priority: Circuit Only Compression Rate: G729 Cordless Support: ○ Enable ● Disable **3** Select the desired settings according to the “Remote Port Configuration field descriptions” on page 171.
network port	do the following: **1** Choose the network port option button on the line of the port number you are configuring. **2** Click the configure button on the same line. **Result:** The Network Port Configuration dialog box appears.  Network Port Configuration Allocation: ○ Permanent ● On Demand PSTN Number: #1234 **3** Select the desired settings according to the “Network Port Configuration field description table” on page 173.
local port	choose the Local TCM option button.

4 To update the MIG RLC with the new information, click Send.

IF you are	THEN
logged on to the MIG RLC	the changes are written into the MIG RLC's buffer. To save the pages in the MIG RLC's Flash memory, complete an Upload/Download → Save to Flash.
not logged on to the MIG RLC	the following dialog box appears:  Configuration Manager Data can't be sent. Connection not Established OK Do one of the following: ■ Log on to the MIG RLC, and then click Send again. ■ Save the changes to a file on your administration PC.

Remote Port Configuration field descriptions

Field	Description
Usage	■ Dedicated: This port is used for one DN only. ■ Multiuser: This port can be time shared by a variety of remote units or different ports on the same remote unit. ■ Dynamic pool: this port is part of a dynamic pool and can be assigned to any remote port requesting access to any port of the MIG RLC pool.

Field	Description
Priority	■ High: This port accesses either the circuit-switched network or the IP network, based on QoS. Calls through High priority ports move to the circuit-switched network first in a QoS transition. In recovery situations, when IP QoS returns to within configured limits, calls through High priority ports return to the IP network last, ensuring the most consistent QoS. ■ Normal: This port accesses either the circuit-switched network or the IP network, based on QoS. Calls through Normal priority ports move to the circuit-switched network only after all calls through High priority ports make the transition. In recovery situations, as QoS on the IP network returns to within configured limits, calls through Normal priority ports return to the IP network first. ■ IP only: This port accesses only the IP network. IP-only channels do not move between networks according to QoS levels. ■ Circuit only: This port accesses only the circuit-switched network (PSTN). Circuit-only channels do not move between networks according to QoS levels.
Compression Rate	Defines the voice quality and network bandwidth afforded to calls on this port.
Cordless Support	■ Enable: This port is providing service only to cordless telephones. ■ Disable: This port is not providing service to cordless telephones. **Note:** Misconfiguration of this field causes incorrect remote telephone operation.

Network Port Configuration field description table

Field	Description
Allocation	■ Permanent: Once a connection is established to the remote unit over this channel, it remains up until the remote unit goes offline. ■ On-demand: The connection to the Remote Office 9150 unit is allowed to go down after it is no longer needed. The connection remains up until the minimum call duration timer expires.
PSTN Number	Enter the telephone number of the remote unit in this field.

Remote connection configuration

Introduction

This section shows you how to choose the following settings for each remote unit:

- security
- the IP connection
- the PSTN connection
- idle timer
- minimum call length timer

Security

The MIG RLC offers three security levels. The following table contains an explanation of each of these levels:

Level	Description
no call security	The MIG RLC permits all incoming calls to access the host PBX regardless of source. **Note:** No call security is the default security level.
caller ID security	The MIG RLC compares the caller ID of the incoming call against the caller IDs entered for this remote unit through the Configuration Manager. If the caller ID does not match any of those entered in this unit's Caller ID table, the MIG RLC denies PBX access to this call.

Level	Description
provisioned security	**1** If the call is from a remote unit to the MIG RLC, the MIG RLC compares the remote unit's outbound security identifier with the inbound security identifier configured for the remote unit on the MIG RLC. If the call is from the MIG RLC to a remote unit, the remote unit compares the MIG RLC's outbound security identifier with the inbound security identifier configured for the MIG RLC on the remote unit. **2** If the compared identifiers match, the receiving end accepts the call. If the compared identifiers do not match, the receiving end rejects the call.

IP connection

If you want to configure a MIG RLC so that it can establish VoIP connections to the Remote Office 9150 unit, you must configure IP functionality for that unit by completing the following steps on the Remote Connection Configuration property sheet:

1 Enable the VoIP functionality on the IP network for that unit by selecting IP Status: Enable.

2 Select IP Configure: Yes.

3 Enter the unit's IP address in the IP Address boxes.

PSTN connection

If you want to configure a MIG RLC so that it can establish circuit-switched connections to the Remote Office 9150 unit, you must configure IP functionality for that unit by completing the following steps on the Remote Connection Configuration property sheet:

1 Enable circuit-switched functionality on the PSTN for that unit by selecting PSTN Status: Enable.

2 Select PSTN Configure: Yes.

3 Enter the unit’s DN in the PSTN Number field.

Timers

Minimum call duration timer

Most ISDN tariffs specify a minimum length of time for which you are charged when you open the line, regardless of the call duration. This is the same as the minimum call charges listed on long distance telephone bills.

The minimum call duration timer is used in circuit-switched mode only and specifies the minimum length of time that each circuit-switched call to the host PBX remains open, regardless of telephone activity or inactivity. The timer should be configured on the MIG RLC to drop the connection just before an additional charge period is incurred. For example, if the timer is set to 59 seconds and your call lasts only 20 seconds, the ISDN connection drops when the timer reaches 59 seconds.

If another call is made to the host PBX before the timer expires, the timer is reset. The timer tracks the last established call.

Idle timer

The idle timer identifies the maximum length of time during which an ISDN connection should remain idle before it can be closed. Idle means that a voice connection does not exist, and buttons are not being pressed on digital telephones.

For example, if the idle timer is set on the MIG RLC to 60 seconds, the ISDN call remains open for 60 seconds after you hang up. Note that if you or someone else dials another number before 60 seconds have passed, another ISDN connection is not opened.

How the timers work to control ISDN costs

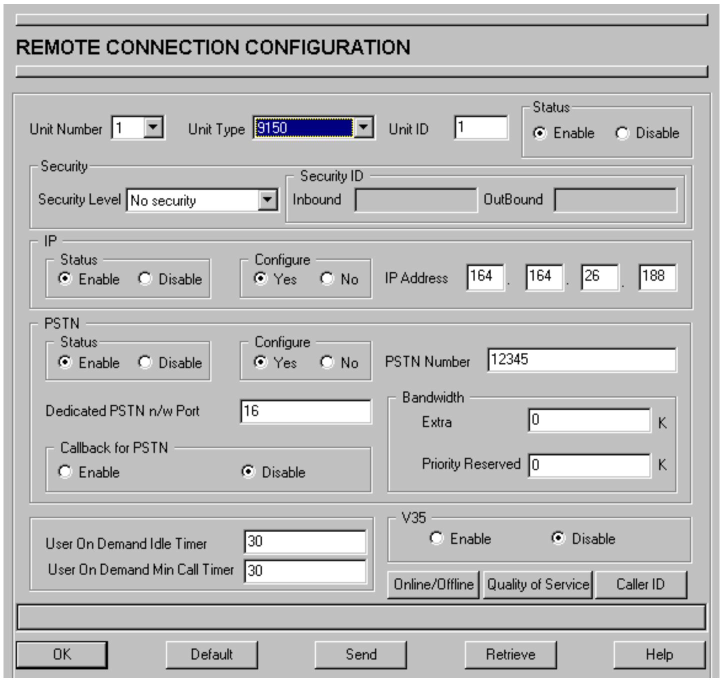
The minimum call duration and idle timers work together to control ISDN charges. The following examples describe what happens when the minimum call duration timer is set to 59 seconds and the idle timer is set to 60 seconds.

Example 1
If the call lasts for 20 seconds and no other calls are made, the ISDN connection drops when the minimum call duration timer reaches 59 seconds. The minimum call duration timer expires before the idle timer.

Example 2
If the call lasts for 65 seconds and no other calls are made, the ISDN connection drops after another 60 seconds have passed without activity. Since the ISDN call exceeded 59 seconds, the minimum call duration timer no longer applies. The idle timer is used in this case to prevent further ISDN charges.

Getting there RLC → Configuration Manager → Remote Connection Configuration

Remote Connection Configuration property sheet



REMOTE CONNECTION CONFIGURATION

Unit Number 1 ▾ Unit Type 9150 ▾ Unit ID 1

Status ● Enable ○ Disable

Security
Security Level No security ▾

Security ID
Inbound
OutBound

IP
Status ● Enable ○ Disable
Configure ● Yes ○ No
IP Address 164 . 164 . 26 . 188

PSTN
Status ● Enable ○ Disable
Configure ● Yes ○ No
PSTN Number 12345

Dedicated PSTN n/w Port 16

Bandwidth
Extra 0 K
Priority Reserved 0 K

Callback for PSTN
○ Enable ● Disable

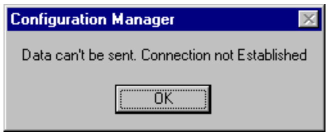
User On Demand Idle Timer 30
User On Demand Min Call Timer 30

V35
○ Enable ● Disable

To configure remote connection settings

1. Complete the fields as described in “Remote Unit Configuration field descriptions” on page 179.
2. Click OK to save the information in the temporary work file.
3. To update the remote unit with the new information, click Send.

IF you are	THEN
logged on to the MIG RLC	the changes are written into the MIG RLC’s buffer. To save the pages in the MIG RLC’s Flash memory, complete an Upload/Download → Save to Flash.

IF you are	THEN
not logged on to the MIG RLC	the following dialog box appears:  Configuration Manager Data can't be sent. Connection not Established OK Do one of the following: ■ Log on to the MIG RLC, and then click Send again. ■ Save the changes to a file on your administration PC.

Remote Unit Configuration field descriptions

Field	Description
Unit Number	Select the site number assigned to the remote unit you are configuring. Valid options: 1–10
Unit Type	Select 9150. **Note:** Only four Remote Office 9150 units can be connected to this MIG RLC.
Unit ID	Enter the unique number between 1–255 assigned to this remote unit. This Unit ID must be different than the MIG RLC's Unit ID and the Unit ID assigned to any other remote unit connected to this MIG RLC. **Note:** This is the same number that is defined as the Unit ID on the 9150 System Configuration property sheet on the Remote Office 9150 unit.
Status	Select Enable to activate the remote unit. Select Disable to deactivate the remote unit.

Field	Description
Security Level	Select the desired security level—no security, caller ID security, or provisioned security. **Note:** See “Meridian Internet Gateway Reach Line Card security” on page 19 for a detailed description of the MIG RLC’s variable security levels.
Security ID: Inbound	If you selected provisioned security, enter the security identifier, up to ten digits in length, that must be presented by calls from the remote unit before they are received at this site.
Security ID: Outbound	If you selected provisioned security, enter the security identifier, up to ten digits in length, that must be presented by calls from the MIG RLC before they are allowed to go out from this site.
IP Status	■ Select Enable to choose the IP network as the primary connection type to the remote unit. ■ Select Disable to disable connectivity to the remote unit over the IP network.
IP Configure	■ Select Enable to configure a static IP address for the remote unit so that the MIG RLC can use it to connect to the remote unit. ■ Select Disable if you do not wish to configure an IP address for the remote unit. **Note:** If you choose not to configure an IP address for the remote unit, the MIG RLC cannot initiate an IP connection between the host and remote sites.
IP Address	Enter the remote unit’s IP address in these fields if you want to be able to initiate the initial IP connection from the MIG RLC.

Field	Description
PSTN Status	■ Select Enable to allow the MIG RLC to connect to the remote unit over the circuit-switched network. ■ Select Disable to prevent the MIG RLC from connecting to the remote unit over the circuit-switched network.
PSTN Configure	■ Select Enable to configure the remote unit’s PSTN number. The MIG RLC dials this number to connect to the remote unit. ■ Select Disable if you do not wish to configure the PSTN number for the remote unit. **Note:** If you choose not to configure a PSTN number for the remote unit, the MIG RLC cannot initiate a circuit-switched network connection between the host and remote sites.
PSTN Number	Enter the PSTN number the MIG RLC must dial to connect to the remote unit.
Dedicated PSTN network port	Enter the MIG RLC network port number that is dedicated to support the remote unit. **Note:** All network ports that are not dedicated are used as a pool to support additional network connections to remote units.
Bandwidth: Extra	Enter the minimum number of kbytes of bandwidth to have available at any time for PSTN access to the remote unit. When the amount of bandwidth available falls below this setting, additional B-channels to the remote unit are opened.
Bandwidth: Priority Reserved	Enter the kbytes of PSTN bandwidth you want to reserve for high priority DNs. High priority DNs consume priority reserved bandwidth before using unreserved bandwidth.

Field	Description
Callback for PSTN	If you enable Callback for PSTN, when the MIG RLC detects a need for increased bandwidth, the MIG RLC sends a signaling message to the remote unit instructing the remote unit to initiate connections on additional trunks to satisfy the need for increased bandwidth. If you disable Callback for PSTN, when the MIG RLC detects a need for increased bandwidth, the MIG RLC initiates connections on additional trunks to satisfy the need for increased bandwidth.
User On Demand Idle Timer	Enter the applicable idle time in seconds. The idle timer identifies the maximum length of time during which an ISDN connection should remain idle before it can be closed. For example, if you set the idle timer to 60 seconds, the ISDN call remains open for 60 seconds after the B-channel is no longer required. See “Idle timer” on page 176.
User On Demand Min Call Timer	Enter the minimum call time in seconds. The minimum call timer specifies the minimum length of time that each ISDN call remains open, regardless of telephone activity (or lack thereof). See “Minimum call duration timer” on page 176.
V.35	For future use.
Online/Offline button	Click to edit the online/offline table for this remote site. See “Configuring an online/offline table” on page 191.
Quality of Service button	Click to edit the QoS settings. See “Quality of Service transitioning technology” on page 163.
Caller ID button	If caller ID security is selected, click to enter caller ID numbers for this remote site.

Configuring Quality of Service

Introduction

This section shows you how to configure the MIG RLC with quality and duration values for QoS transitioning technology. The settings configured here apply to both the MIG RLC and the remote unit.

When voice quality on the IP network falls below the specified threshold and duration values, calls are moved from the IP network to the circuit-switched network. For further details, see “Configurable Quality of Service transitioning technology” on page 13.

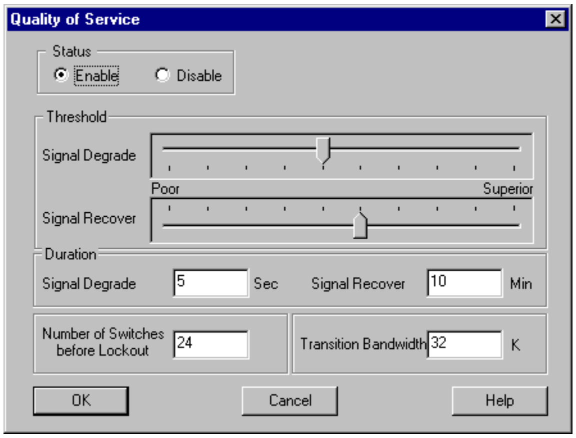
More information

To determine the appropriate QoS settings for your IP network, see Appendix A, “Network engineering guidelines.”

Getting there

RLC → Configuration Manager → Remote Connection Configuration → Quality of Service

Quality of Service dialog box



Quality of Service

Status: ● Enable ○ Disable

Threshold

Signal Degrade

Signal Recover

Duration

Signal Degrade 5 Sec

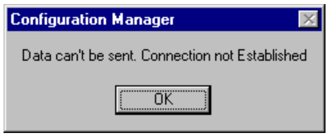
Signal Recover 10 Min

Number of Switches before Lockout 24

Transition Bandwidth 32 K

To configure the Quality of Service

1. Complete the fields as described in “Quality of Service field descriptions” below.
2. Click OK to save the information in the temporary work file.
3. To update the remote unit with the new information, click Send.

IF you are	THEN
logged on to the MIG RLC	the changes are written into the MIG RLC’s buffer. To save the pages in the MIG RLC’s Flash memory, complete an Upload/Download → Save to Flash.
not logged on to the MIG RLC	the following dialog box appears:  Configuration Manager Data can't be sent. Connection not Established OK Do one of the following: ■ Log on to the MIG RLC, and then click Send again. ■ Save the changes to a file on your administration PC.

Quality of Service field descriptions

Field	Description
Status	■ Select Enable to allow QoS transitions to occur when the QoS on the IP network degrades. ■ Select Disable if you do not want to use the QoS transitioning technology.
Threshold: Signal Degrade	Move the indicator to the appropriate point on the sliding scale, a relative value between poor and superior.

Field	Description
Threshold: Signal Recover	Move the indicator to the appropriate point on the sliding scale, a relative value between poor and superior.
Duration: Signal Degrade	Enter a value, in seconds, between 1 and 60. If poor voice quality lasts for the specified duration, then calls are moved from the IP network to the circuit-switched network.
Duration: Signal Recover	Enter a value, in minutes, between 1 and 10. When the improved voice quality lasts for the duration value chosen (in seconds), then calls are moved back to the IP network.
Number of Switches before Lockout	Enter the number of transitions that must occur between the IP and circuit-switched networks before the MIG RLC stops making the transition.
Transition Bandwidth	Specify the amount of bandwidth to be reserved for transitions.

Section C: Online/offline table

In this section

How the online/offline table works

Introduction

The online/offline table is the schedule of times at which an ISDN connection is available to a remote site. The online/offline table gives you the ability to ensure that the costly ISDN connection is disabled after business hours.

The remote site has the ability to override the settings of the online/offline table should the table attempt to suspend access to the ISDN connection in the middle of a call. Each user station at the remote site is alerted by a buzz 30, 20, and 10 seconds before the connection is terminated. Each user at the remote site has the opportunity to enter the applicable SPRE code on his or her telephone key pad during the 30-second alert period to override the termination of the connection.

Notes:

- The online/offline table does not prevent a user from establishing or terminating a connection to the network.
- When the remote unit is in the offline mode, remote-unit users cannot make host-controlled calls over the IP or circuit-switched networks.

Online/offline configuration example

The online/offline table allows you to enter up to eight entries per day, every day of the week, for each remote site. The following is an example of a configured online/offline schedule for a MIG RLC channel:

Entry	State	State
Entry 1	At 8:00 a.m., the MIG RLC establishes the remote site’s ISDN connection.	Online
Entry 2	At 11:30 a.m. (a common lunchtime), the MIG RLC terminates the ISDN connection.	Offline

Entry	State	State
Entry 3	At 12:30 p.m. (the end of lunchtime), the MIG RLC reestablishes the ISDN connection.	Online
Entry 4	At 5:00 p.m., the MIG RLC terminates the ISDN connection for the day.	Offline

Online/offline table overrides

Any remote site user can override the settings of the online/offline table should the table attempt to suspend access to the ISDN connection in the middle of a call. A buzz alerts users at the remote site that the ISDN connection is about to go down. After the initial warning, users can enter the applicable SPRE code on their telephone key pads to override the termination of the connection. The warning buzz repeats itself 20 and 10 seconds before the connection is terminated. Any user can enter the online SPRE code to avoid going offline.

Multiple offline periods

Multiple offline periods can be entered into the table without interrupting online periods. In this way, you can program the MIG RLC to terminate a connection that has been left open should a remote site user be forced to override a scheduled ISDN termination.

For example, Mr. Smith, a remote site user, begins a business call with Mr. Jones, Mr. Smith’s customer, at 4:45 p.m. The MIG RLC is programmed to terminate his ISDN connection at 5:00 p.m. However, Mr. Smith overrides the scheduled termination, and the call goes on for another 45 minutes. The business call is a success, but the expensive ISDN connection is still up and, if the usual schedule were followed, would not be terminated until lunchtime the next day.

Fortunately, Mr. Smith’s system administrator foresaw this situation and configured offline commands for 6:00, 7:00, and 8:00 p.m. So, the ISDN connection is terminated at 6:00 p.m., and only 15 minutes of unnecessary ISDN charges are accrued by Mr. Smith’s company.

What happens when an offline entry is processed

When the MIG RLC processes an offline entry, the MIG RLC instructs the remote unit to go offline for a specified number of hours and minutes. The number of hours and minutes the remote unit remains offline is the difference between the offline entry being processed and the next online entry.

For example, an offline entry is configured at 6:00 p.m. The next online entry is configured at 9:00 a.m. the next day. When the MIG RLC processes the 6:00 p.m. offline entry, it instructs the remote unit to go offline for 15 hours.

If someone wants to reach the remote site user while the digital telephone is in offline mode, the caller must dial the ISDN number assigned to the digital telephone.

How the remote site goes back online

When going offline, the remote unit’s offline timer is activated. When the timer expires (in the example above, this is at 9:00 a.m.), the remote unit automatically initiates a “going online” request to the PBX. If the MIG RLC successfully receives the request, the remote site and its associated digital telephones go online.

Implications

If the online/offline table contains only offline entries (no online entries are configured), then the MIG RLC instructs the remote unit to go offline forever each time an offline entry is processed. To go back online, a remote user must enter the online SPRE code to make host-controlled calls on either the IP or circuit-switched network.

Configuring an online/offline table

Introduction

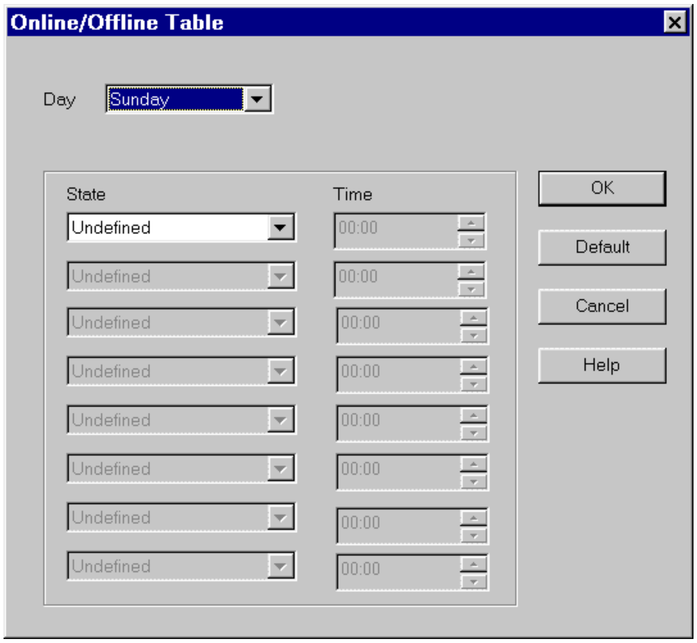
This section describes how to configure an online/offline table for remote units.

The online/offline table allows you to enter up to eight entries per day, every day of the week, for each remote site. You can define each entry as online, offline, or undefined for each time period entered.

Getting there

RLC → Configuration Manager → Online/Offline Table

Online/Offline Table sheet



Day: Sunday

State	Time
Undefined	00:00
Undefined	00:00
Undefined	00:00
Undefined	00:00
Undefined	00:00
Undefined	00:00
Undefined	00:00
Undefined	00:00

To configure the online/offline table

1. In the Day list box, select the day of the week for which you want to schedule an online/offline table.
2. In the State list box beside Entry 1, do one of the following:

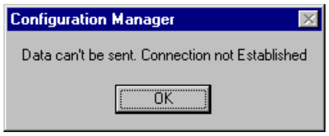
To	Select
activate the connection to the remote port at the time specified in step 3	Online.
terminate the connection to the remote port at the time specified in step 3	Offline.
remove online or offline states	Undefined.

3. In the Time scroll box beside Entry 1, enter the start time for the day's schedule.
4. Repeat steps 2 and 3 in the remaining entry fields to complete the daily schedule.

   Note: The table allows you to enter up to eight schedule entries per day, every day of the week, for up to ten remote sites.

5. Click OK to save the information in the temporary work file.
6. To update the remote unit with the new information, click Send.

IF you are	THEN
logged on to the MIG RLC	the changes are written into the MIG RLC's buffer. To save the pages in the MIG RLC's Flash memory, complete an Upload/Download → Save to Flash.

IF you are	**THEN**
not logged on to the MIG RLC	the following dialog box appears:  Data can't be sent. Connection not Established Do one of the following: ■ Log on to the MIG RLC, and then click Send again. ■ Save the changes to a file on your administration PC.

Chapter 7

Administration

In this chapter

Overview

Introduction

This chapter provides procedures for administration of the Meridian Internet Gateway Reach Line Card (MIG RLC).

Changing the administration password

The MIG RLC's configuration is protected by two layers of password security. If you want to secure the MIG RLC's configuration so that others cannot tamper with it, change the following items:

- Configuration Manager password

  This password prevents unauthorized offline configuration changes.
- MIG RLC's password

  This password prevents unauthorized online changes of the configuration residing in the MIG RLC's flash memory.

See page 198 for information on customizing the password.

Performing backups and restores

For the procedures necessary to back up configuration files as a part of day-to-day operation, refer to "Storing backup configuration files" on page 207. For information on how to restore a configuration file, see "To upload a configuration to a unit" on page 134.

System logs

The MIG RLC keeps track of system performance through the maintenance of logs. The Configuration Manager gives you several ways of working with these logs to get the information you need to keep your remoting system operating at its peak. See page 215 for more information on working with the MIG RLC's system logs.

Viewing statistics

In addition to the information kept in logs, the MIG RLC collects statistical data about system operation and usage. The section beginning on page 221 provides you with information on viewing and interpreting those statistics.

Performing upgrades

Nortel Networks is constantly working on enhanced functionalities for existing products. As these new functionalities are developed, they are made available to existing customers in the form of software upgrades. This section provides information on how to obtain these new functionalities as they are made available and how to add them to your system.

Changing the administration password

Introduction

The MIG RLC’s configuration is protected by two layers of password security. If you want to secure the MIG RLC’s configuration so that others cannot make configuration changes, alter the following items:

- the Configuration Manager password

  This password prevents unauthorized offline configuration changes from being performed.
- the MIG RLC’s password

  This password prevents unauthorized online changes of the configuration residing in the MIG RLC’s flash memory.

ATTENTION

Ensure that you record the passwords and store them in a safe, secure place. If you forget or lose the password, you must contact your Nortel Networks technical support representative.

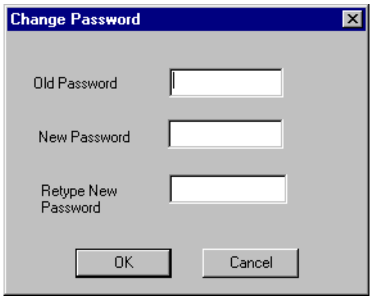
Getting there

RLC → Configuration Manager

To change the Configuration Manager password

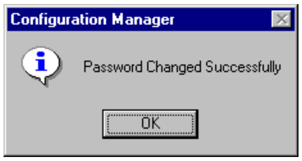
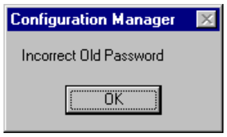
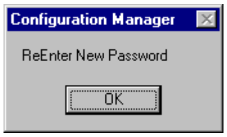
1 Choose Connect → Change Password → Local.

Result: The Change Password dialog box appears.



2 Complete the fields as described in “Password dialog box field descriptions” on page 201.

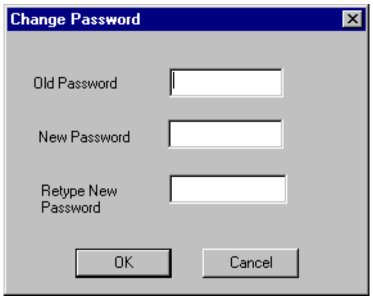
3 Click OK.

IF the password change	THEN
was successful	the following message appears:  Password Changed Successfully Click OK.
was not successful	one of the following messages appears:  Incorrect Old Password  ReEnter New Password Click OK, then return to step 2.

To change the MIG RLC’s password

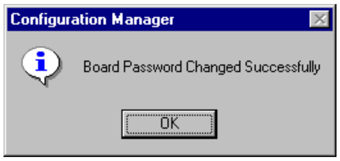
1 Choose Connect → Change Password → Board.

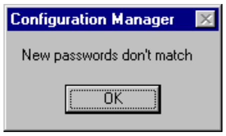
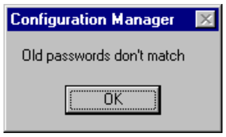
Result: The Change Password dialog box appears.



2 Complete the fields as described in “Password dialog box field descriptions” on page 201.

3 Click OK.

IF the password change	THEN
was successful	the following message appears:  Board Password Changed Successfully **Note:** This means the password has been written to the MIG RLC’s flash memory. Click OK.

IF the password change	THEN
was not successful	one of the following messages appear.:  New passwords don't match  Old passwords don't match Click OK, then return to step 1.

4 From the menu, choose Upload/Download → Save to Flash.

Result: The MIG RLC's memory is updated with the new password.

5 Restart the MIG RLC.

Password dialog box field descriptions

Field	Description
Old Password	Enter the existing password.
New Password	Enter the new password.
Retype New Password	Enter the new password again.

Using the XConnect command for PBX maintenance from a remote site

Introduction

This section shows you how to establish a connection to the PBX’s serial data interface (SDI) port from a remote site. First, you must log on to the MIG RLC via Telnet. With this connection established, remote-site system administrators can perform PBX maintenance procedures.

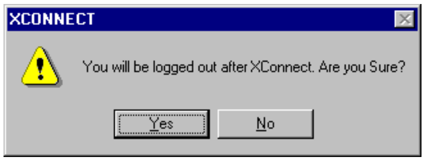
Getting there RLC → Configuration Manager

To connect to the PBX’s SDI port from a remote site

1 Log on to the MIG RLC using Telnet.

2 Choose Connect → XConnect.

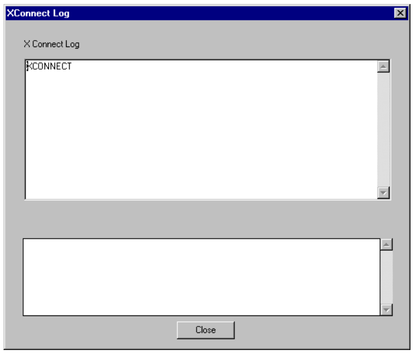
Result: Configuration Manager warns you that if you continue, you will be logged off the logged-on unit after you end your SDI session.



XCONNECT

You will be logged out after XConnect. Are you Sure?

3 Choose how you wish to continue from the choices in the following table:

IF you want to	THEN
establish a connection to the PBX’s SDI port even though ending your PBX maintenance session will close your connection with the logged-on unit	do the following: **a** Click Yes. **Result:** Configuration Manager establishes the serial connection from the MIG RLC to the PBX’s SDI port and presents you with the XConnect Log screen.  XCONNECT **b** Conduct the required PBX maintenance activities. **c** When you are ready to end your PBX configuration session, click Close. **Result:** Configuration Manager closes the serial connection to the PBX’s SDI port and logs you off the MIG RLC.
keep your connection to the logged-on unit	click No. **Result:** The dialog box closes.

Section A: Performing backups and restores

In this section

Overview

Introduction

This section describes how to create a backup copy of the MIG RLC’s configuration. It also describes how to use this backup copy to restore the configuration.

How a backup file is created

You create a backup copy of the MIG RLC’s configuration by downloading the MIG RLC’s configuration from flash memory to a text file on your administration PC.

How restores are done

You restore the MIG RLC’s configuration in flash memory by uploading a configuration text file from your administration PC.

The upload is performed over the IP network using the TFTP protocol. You must have a TFTP server application running on your administration PC.

Creating a backup configuration file

Introduction

Create a backup copy of the MIG RLC’s configuration by downloading the MIG RLC’s configuration from flash memory to a text file on your administration PC.

When to create a backup

Nortel Networks recommends that you create a backup of your configuration file whenever you make configuration changes or after you perform a firmware upgrade.

Storing backup configuration files

The MIG RLC is an extension of the telecommunications and data network. It is extremely important that you keep a backup copy of the MIG RLC’s configuration. If the MIG RLC’s flash memory or configuration becomes corrupted or is lost, you can easily restore it.

Store the configuration file in a safe, secure location, such as on backup tape or other media that is stored offsite.

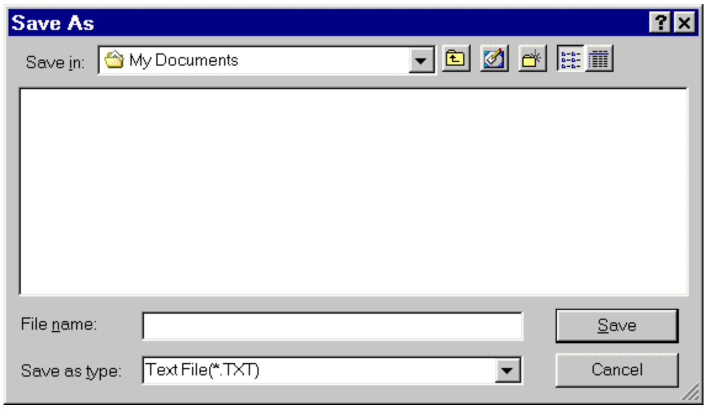
Nortel Networks recommends that you keep the backup files indefinitely.

Getting there RLC → Configuration Manager

To create the backup file

1 From the menu, choose Upload/Download → Download Configuration.

Result: The Save As dialog box appears.



2 Navigate to the folder where you want to put the configuration text file.

3 Enter a name for the file in the File name box.

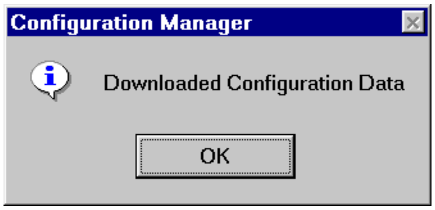
Note: This configuration file will become your backup file, so ensure the file name is meaningful. The file name's extension is .TXT.

4 Click Save.

Result: The Save As box closes, and the following message appears in the status bar at the bottom of the screen:

```
Downloading Config From Board
```

When completed, the following appears:



Downloaded Configuration Data

5 Click OK.

Restoring the configuration

Introduction

Restore the MIG RLC’s configuration in flash memory by uploading a configuration text file from your administration PC.

The upload is performed over the IP network using the TFTP protocol. You must have a TFTP server application running on your administration PC. The TFTP server’s base directory must point to the directory that contains the configuration file you want to upload.

Before you begin

Before you can upload the configuration file to the MIG RLC, you must do the following:

1 Start the TFTP server application.

2 Ensure the TFTP base directory reflects the directory where the configuration file you want to upload is located.

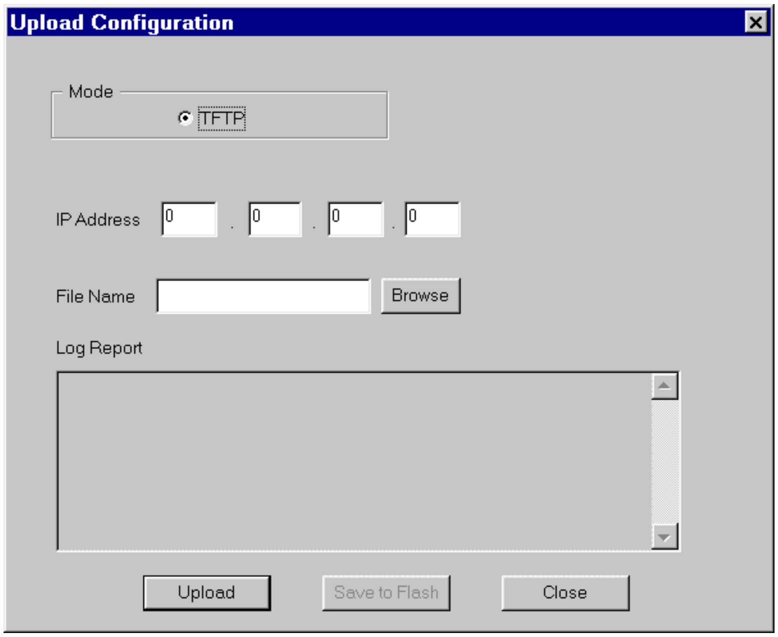
Getting there

RLC → Configuration Manager

To upload a configuration file over the IP network

1 From the menu, choose → Upload/Download → Upload Configuration

Result: The Upload Configuration screen appears.



Mode
● TFTP

IP Address 0 . 0 . 0 . 0

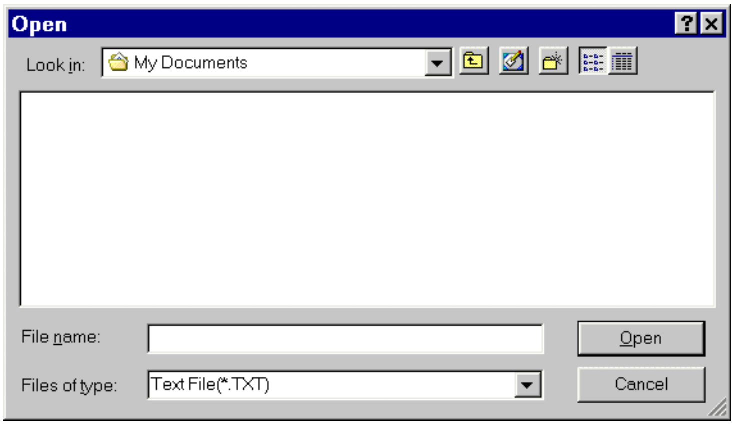
File Name

2 In the IP Address boxes, enter the IP address of the TFTP server.

Note: Since the TFTP server application is running on your administration PC, this is the IP address of the PC.

3 Click Browse.

Result: The Open dialog box appears.



4 Ensure the Files of type box shows Text File(*.TXT).

5 Navigate to the folder in which the the configuration file is located.

6 Select the file, and then click Open.

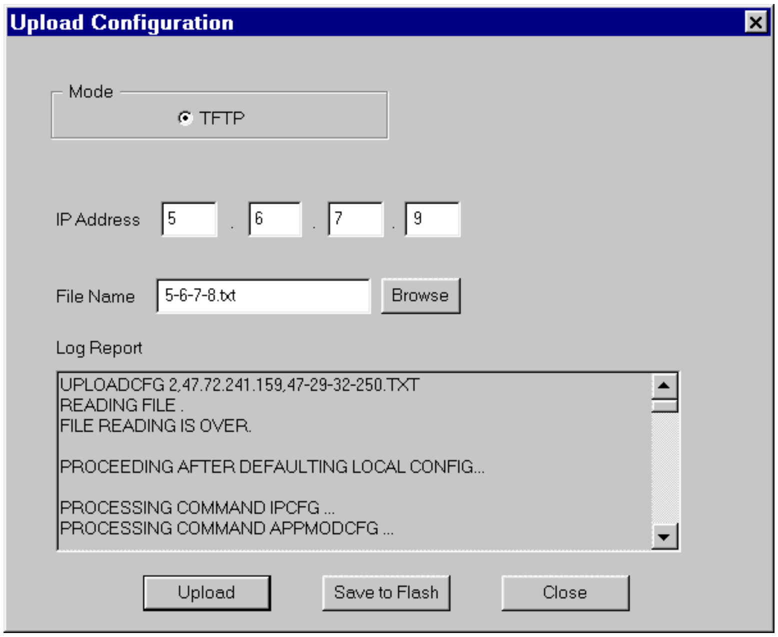
Result: You are returned to the Upload Configuration dialog box. The file you selected is shown in the File Name box.

7 Click Upload.

Result: If the file opens successfully, then the upload proceeds. The following message appears in the status bar at the bottom of the screen:

```
Uploading Config to Board
```

Status messages relating to the upload appear in the middle of the Upload Configuration dialog box. The following is an example.



Mode: ● TFTP

IP Address: 5 . 6 . 7 . 9

File Name: 5-6-7-8.txt

Log Report

```
UPLOADCFG 2,47.72.241.159,47-29-32-250.TXT
READING FILE .
FILE READING IS OVER.

PROCEEDING AFTER DEFAULTING LOCAL CONFIG...

PROCESSING COMMAND IPCFG ...
PROCESSING COMMAND APPMODCFG ...
```

CAUTION

Risk of incorrect operation due to partial configuration

Do not interrupt the configuration upload. If you interrupt the configuration upload, this results in an incomplete configuration in the MIG RLC's database.

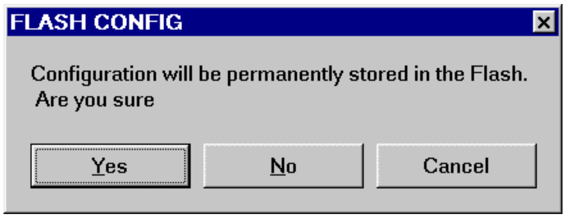
If the configuration upload is interrupted, repeat this procedure immediately.

IF the upload was	THEN
successful	The following message appears: `CONFIG UPLOAD SUCCESSFUL... USE SAVECFG TO UPDATE FLASH.` Go to step 8.

IF the upload was	THEN
not successful	the following message appears in the middle of the Upload Configuration dialog box: `CONFIG UPLOAD FAILED` For further instructions, see Chapter 8, “Troubleshooting.”

8 On the Upload Configuration screen, click Save to Flash.

Result: The following dialog box appears:



FLASH CONFIG

Configuration will be permanently stored in the Flash.
Are you sure

9 Click Yes.

Result: The following message appears in the status bar at the bottom of the screen:

```
Saving to Flash in Progress
```

When the save is finished, the following message appears in the middle of the Upload Configuration dialog box:

```
CONFIGURATION IS UPDATED INTO FLASH...
```

10 Click Close.

11 Restart the MIG RLC.

Note: For instructions, see “Performing a system restart or shutdown” on page 146.

Section B: System logs

In this section

Overview

Introduction

The MIG RLC keeps track of system performance through the maintenance of logs. The Configuration Manager gives you several ways of working with these logs to get the information you need to keep your remoting system operating at its peak.

Displaying logs

For logs to be useful, you must be able to see the information they hold. You can use the procedure on page 217 to view that information.

Resizing logs

You might find that you want MIG RLC logs to occupy a larger or smaller percentage of disk space on your administration PC. The procedure described on page 219 allows you to change the size of the logs the MIG RLC maintains.

Clearing logs

The MIG RLC allows you to save disk space by clearing the log queue whenever you wish to do so. You can use the procedure described on page 220 to discard information from the logs that is no longer useful.

Displaying logs

Introduction

The MIG RLC keeps track of system performance through the maintenance of logs. Each line stored in the log represents a separate action completed by the unit.

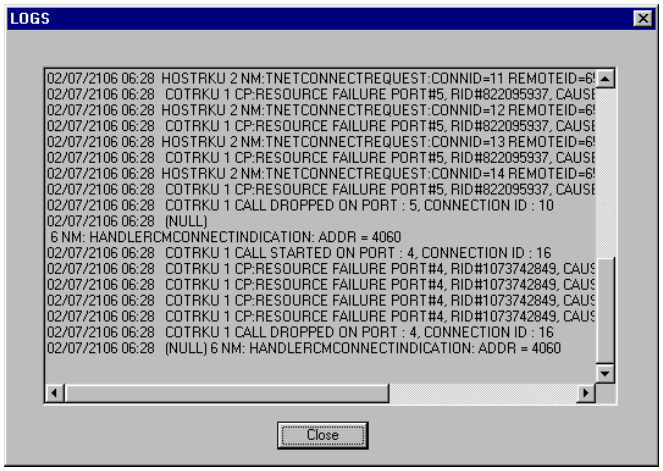
Use these logs when you want to troubleshoot system problems. You can print the log to a text file by copying the information from the log window, and then pasting it into a text file.

Getting there RLC → Configuration Manager

To display logs

From the menu, choose Alarms/Stats/Logs → Display Logs.

Result: The MIG RLC displays the logs it maintains in a window similar to the following. You can use the scroll bar to browse through the logs to find the information in which you are interested.



```
02/07/2106 06:28  HOSTRKU 2 NM:TNETCONNECTREQUEST:CONNID=11 REMOTEID=6
02/07/2106 06:28   COTRKU 1 CP:RESOURCE FAILURE PORT#5, RID#822095937, CAUSE
02/07/2106 06:28  HOSTRKU 2 NM:TNETCONNECTREQUEST:CONNID=12 REMOTEID=6
02/07/2106 06:28   COTRKU 1 CP:RESOURCE FAILURE PORT#5, RID#822095937, CAUSE
02/07/2106 06:28  HOSTRKU 2 NM:TNETCONNECTREQUEST:CONNID=13 REMOTEID=6
02/07/2106 06:28   COTRKU 1 CP:RESOURCE FAILURE PORT#5, RID#822095937, CAUSE
02/07/2106 06:28  HOSTRKU 2 NM:TNETCONNECTREQUEST:CONNID=14 REMOTEID=6
02/07/2106 06:28   COTRKU 1 CP:RESOURCE FAILURE PORT#5, RID#822095937, CAUSE
02/07/2106 06:28   COTRKU 1 CALL DROPPED ON PORT : 5, CONNECTION ID : 10
02/07/2106 06:28   (NULL)
 6 NM: HANDLERCMCONNECTINDICATION: ADDR = 4060
02/07/2106 06:28   COTRKU 1 CALL STARTED ON PORT : 4, CONNECTION ID : 16
02/07/2106 06:28   COTRKU 1 CP:RESOURCE FAILURE PORT#4, RID#1073742849, CAUS
02/07/2106 06:28   COTRKU 1 CP:RESOURCE FAILURE PORT#4, RID#1073742849, CAUS
02/07/2106 06:28   COTRKU 1 CP:RESOURCE FAILURE PORT#4, RID#1073742849, CAUS
02/07/2106 06:28   COTRKU 1 CP:RESOURCE FAILURE PORT#4, RID#1073742849, CAUS
02/07/2106 06:28   COTRKU 1 CALL DROPPED ON PORT : 4, CONNECTION ID : 16
02/07/2106 06:28   (NULL) 6 NM: HANDLERCMCONNECTINDICATION: ADDR = 4060
```

Note: The information displayed in these logs also appears in the event.dat file on your administration PC.

To print the log to a file

If you are requesting technical support, you might be asked to provide a copy of the logs. To recreate the log in a file on your administration PC, follow this procedure:

1. Position the mouse pointer inside the log window at the beginning of the text you want to copy.
2. Select the text you want to copy, and then press Ctrl-C.
3. Open WordPad or Notepad.
4. Press Ctrl-V to paste the text.
5. Save and close the text file.

Resizing logs

Introduction

The log maintains a maximum of 1000 lines of text. When the log reaches 1000 text lines, new text lines overwrite existing lines.

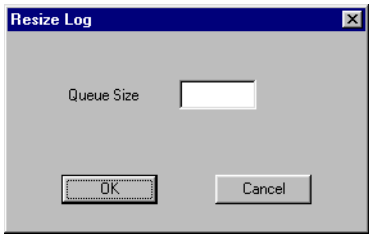
You might find that you want the logs to occupy a larger or smaller percentage of memory on the MIG RLC. You can use the following procedure to change the size of the logs that the MIG RLC keeps.

Getting there RLC→ Configuration Manager

To change the size of MIG RLC logs

1 From the menu, choose Alarms/Stats/Logs → Resize Logs.

Result: The MIG RLC gives you the option of selecting the size of the queue in which the logs are held.



Note: The queue size, in this case, means the number of text lines in the log. The log currently holds a maximum of 1000 text lines.

2 Enter the maximum number of text lines you want to maintain in the log.

3 Click OK.

Clearing logs

Introduction

The MIG RLC allows you to save disk space by clearing the log queue. Use the following procedure to discard information from the logs that is no longer useful.

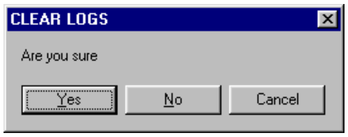
Getting there RLC → Configuration Manager

To clear logs

1 Choose the Alarms/Stats/Logs pull-down menu in the menu bar.

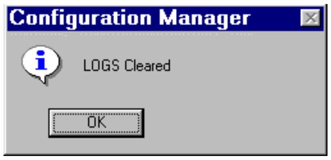
2 Select the Clear Logs option.

Result: The MIG RLC presents a screen similar to the following screen:



CLEAR LOGS

Are you sure

IF you select	THEN
No or Cancel	the dialog box disappears and returns you to the blank Configuration Manager screen.
Yes	the MIG RLC logs are cleared and the following confirmation screen appears:  Configuration Manager LOGS Cleared OK

Section C: Viewing statistics

In this section

Overview

Introduction

In addition to the information kept in logs, the MIG RLC collects statistical data about system operation and usage. This section provides you with information on viewing and interpreting those statistics.

Trunk Connection Statistics screen

The Trunk Connection Statistics screen allows you to see the amount of traffic that is processed over each B-channel. Use these statistics to determine which trunks get used the most. The elements of this group include

- trunk number
- remote ID
- called number
- up time
- close time
- duration

To view the Trunk Connection Statistics screen, follow the procedure on page 225.

Bandwidth Connection Statistics screen

The Bandwidth Connection Statistics screen allows you to see how much bandwidth is actually being used, and how much bandwidth is available. Use these statistics to help you determine if you need to add more bandwidth on the circuit-switched network or IP connections. The elements of this group include

- remote unit number
- active connections
- active logical trunks
- total trunk BW
- used trunk BW

- used IP BW
- total possible BW

To view the Bandwidth Connection Statistics screen, follow the procedure on page 227.

Caller Information Statistics screen

The Caller Information Statistics screen allows you to see the types of calls being made (IP or circuit-switched), and how often QoS transitions occur. Use this statistics log to help you determine if the QoS on your IP network is stable. The elements of this group include

- call number
- remote ID
- current media
- priority
- connection state
- call BW
- start time
- switch trunk number
- switch IP number
- last transition to PSTN
- last transition to IP

To view the Caller Information Statistics screen, follow the procedure on page 231.

Hardware Statistics screen

The Hardware Statistics screen lists the modules that are installed on the MIG RLC. Use it to determine which module positions are populated, and what they contain. The elements of this group include

- module number
- module type
- DSP type

To view the Hardware Statistics screen, follow the procedure on page 236.

Trunk Connection Statistics screen

Introduction

The trunk connection statistics allow you to see the amount of traffic that is processed over each B-channel. Use these statistics to determine which trunks get used the most.

Getting there

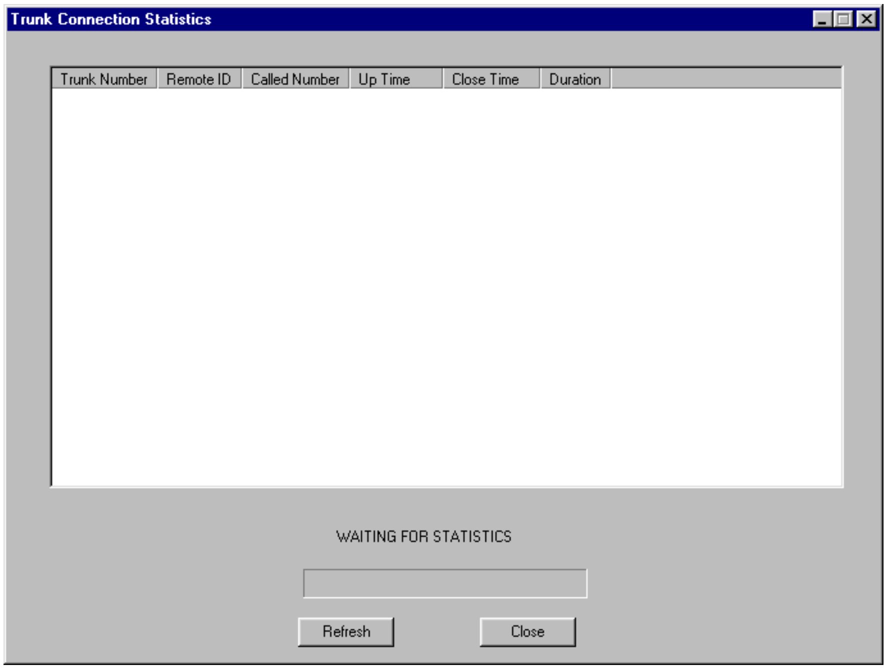
RLC → Configuration Manager

To display the trunk connection statistics

1 Choose Alarms/Stats/Logs → Trunk Connection Statistics.

2 Wait while Configuration Manager gathers statistics from the MIG RLC's system logs.

Result: The statistics appear in a window similar to the following:



WAITING FOR STATISTICS

3 Do one of the following options:

- To refresh the statistics, click Refresh.
- To close the statistics window, click Close.

Trunk Connection Statistics field descriptions

Column	Description
Trunk Number	Identifies the trunk used by the call.
Remote ID	Identifies the Remote Office 9150 unit involved in the call.
Called Number	Identifies the telephone number receiving the call.
Up Time	Identifies the time at which the call began.
Close Time	Identifies the time at which the call ended.
Duration	Identifies how long the call has lasted.

Bandwidth Connection Statistics screen

Introduction

The Bandwidth Connection Statistics screen allows you to see how much bandwidth is actually being used, and how much bandwidth is available. Use these statistics to help you determine if you need to add more bandwidth on the circuit-switched network or IP connections. The elements of this group include

- remote unit number
- active connections
- active logical trunks
- total trunk BW
- used trunk BW
- used IP BW
- total possible BW

To view bandwidth connection statistics, follow the procedure below.

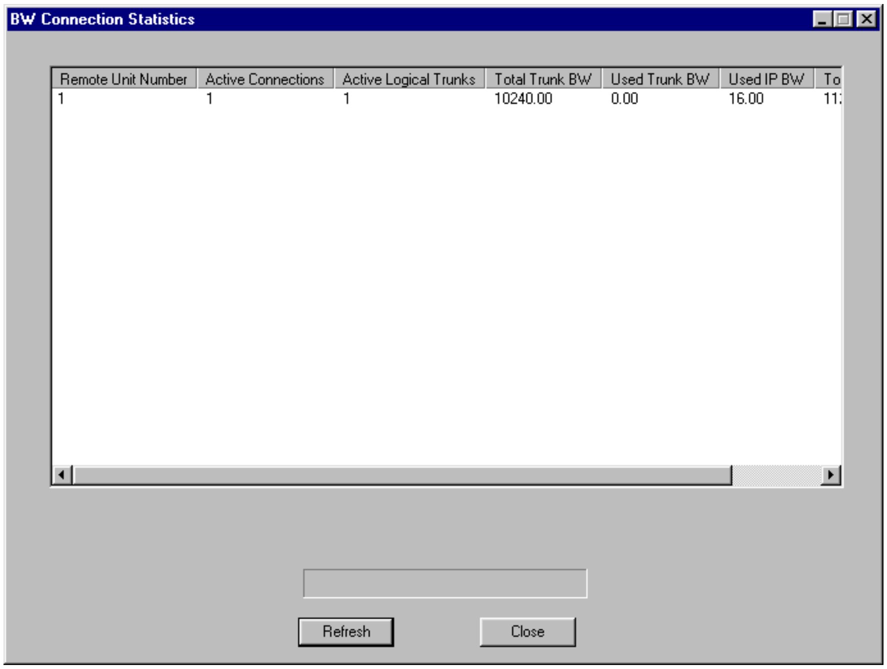
Getting there

RLC → Configuration Manager

To display the bandwidth connection statistics

1. Choose Alarms/Stats/Logs → BW Connection Statistics.
2. Wait while Configuration Manager gathers statistics from the MIG RLC’s system logs.

   Result: The statistics appear.



Remote Unit Number	Active Connections	Active Logical Trunks	Total Trunk BW	Used Trunk BW	Used IP BW	To
1	1	1	10240.00	0.00	16.00	11

3 Do one of the following options:

- To refresh the statistics, click Refresh.
- To close the statistics window, click Close.

BW Connection Statistics field descriptions

Column	Description
Remote Unit Number	Identifies the Remote Office 9150 unit that initiated the call.
Active Connections	Identifies the number of calls currently in progress.
Active Logical Trunks	Identifies the number of other Remote Office 9150 units or MIG RLCs to which the logged on unit is connected.

Column	Description
Total Trunk BW	Identifies the possible circuit-switched bandwidth of the logged on unit.
Used Trunk BW	Identifies the circuit-switched bandwidth currently in use.
Used IP BW	Identifies the IP bandwidth currently in use.
Total Possible Bandwidth	Identifies the possible combined circuit-switched and IP bandwidth of the logged on unit.

Caller Information Statistics screen

Introduction

The Caller Information Statistics screen allows you to see the types of calls being made (IP or circuit-switched), and how often QoS transitions occur. Use this statistics log to help you determine if the voice QoS on your IP network is stable. The elements of this group include

- call number
- remote ID
- current media
- priority
- connection state
- call BW
- start time
- switch trunk number
- switch IP number
- last transition to PSTN
- last transition to IP

To view caller information statistics, follow the procedure below.

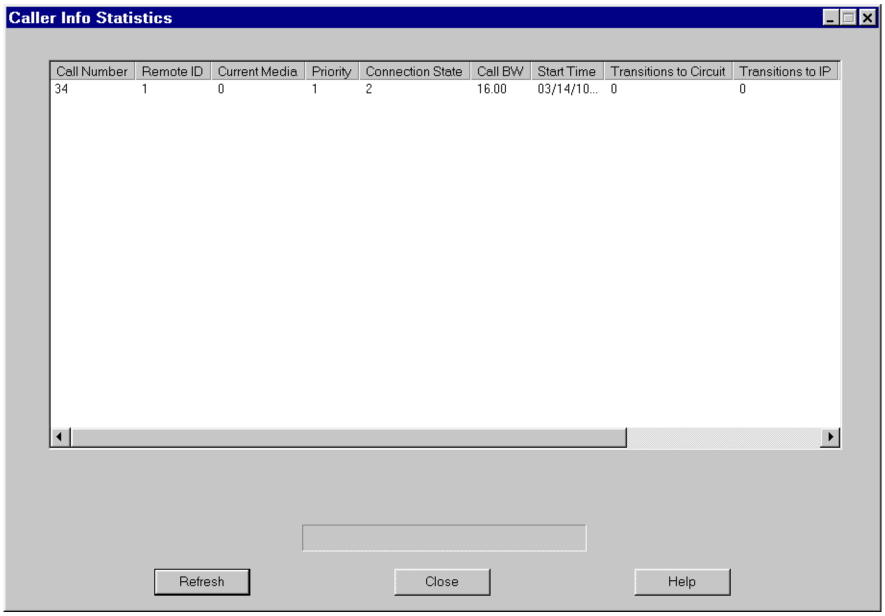
Getting there RLC → Configuration Manager

To display the caller information statistics

1 Choose Alarms/Stats/Logs → Caller Info Statistics.

2 Wait while Configuration Manager gathers statistics from the MIG RLC's system logs.

Result: The statistics appear in a window similar to the following:



Caller Info Statistics

Call Number	Remote ID	Current Media	Priority	Connection State	Call BW	Start Time	Transitions to Circuit	Transitions to IP
34	1	0	1	2	16.00	03/14/10...	0	0

3 Do one of the following options:

- To refresh the statistics, click Refresh.
- To close the statistics window, click Close.

Caller Info Statistics field descriptions

Column	Description
Call Number	Identifies the unique number of this call through the lifetime of the logged on unit.
Remote ID	Identifies the unit ID of the involved remote unit.

Column	Description
Current Media	Identifies whether the call is placed over the circuit-switched or IP network.
Priority	Identifies the priority setting of the involved trunk (circuit-switched only, IP only, high, or normal).
Connection State	Identifies whether the call is currently up.
Call BW	Identifies how much bandwidth was used by the call.
Start Time	Identifies the time at which the connection was initiated.
Transitions to Circuit	Identifies the number of times the call was switched to the circuit-switched network.
Transitions to IP	Identifies the number of times the call was switched to the IP network.
Last Transition to PSTN	Identifies the last time the call was switched from the IP network to the circuit-switched network.
Last Transition to IP	Identifies the last time the call was switched from the circuit-switched network to the IP network.

Voice Connection Table

Introduction

The Voice Connection Table (VCT) statistics screen contains certain properties of the connections that are active at the time that you request the statistics. Technical support personnel use these statistics for troubleshooting purposes. The elements of the VCT statistics group include

- connection ID
- remote ID
- RLC port number
- remote port number
- RCM callback pointer
- DSP callback pointer
- start time
- duration

For definitions of these statistics, see “VCT Statistics field descriptions” on page 234. To view VCT statistics, follow the procedure below.

Getting there

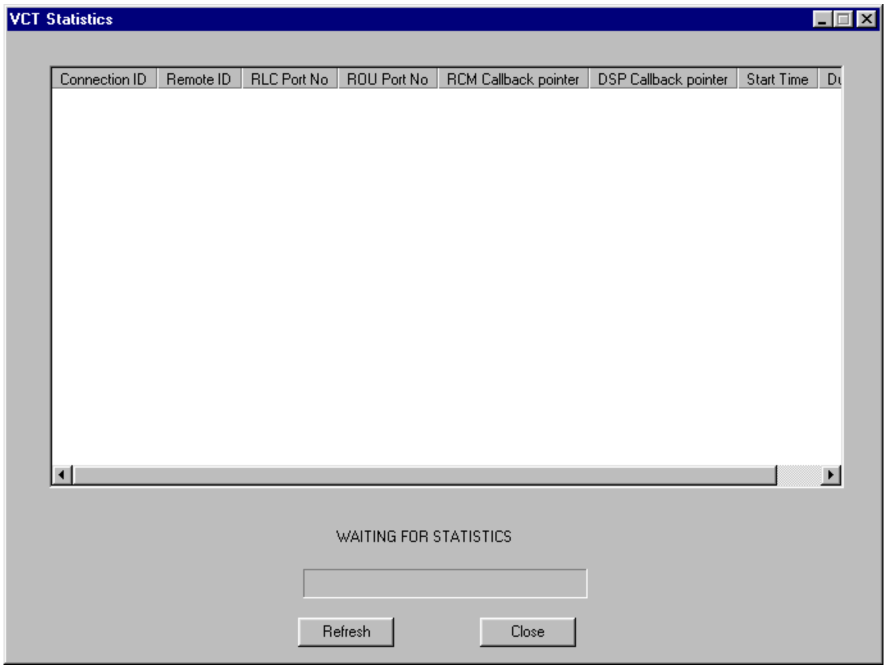
RLC → Configuration Manager

To display the VCT Statistics screen

1 Choose Alarms/Stats/Logs ➝ VCT.

2 Wait while Configuration Manager gathers statistics from the MIG RLC’s system logs.

Result: The statistics appear in a window similar to the following:



3 Do one of the following options:

- To refresh the statistics, click Refresh.
- To close the statistics window, click Close.

VCT Statistics field descriptions

Column	Description
Connection ID	A sequential number used for tracking individual calls.
Remote ID	Identifies the unit ID of the involved remote unit.

Column	Description
RLC Port No.	Identifies the port through which the call was processed at the host site.
ROU Port No.	Identifies the port through which the call was processed at the remote site.
RCM Callback pointer	Identifies the address of a programming routine for technical support use.
DSP Callback pointer	Identifies the address of a programming routine for technical support use.
Start Time	Identifies the time and date when the call started.
Duration	Identifies how long the call lasted.

Hardware Statistics screen

Introduction

The Hardware Statistics screen lists the modules that are installed on the MIG RLC. Use it to determine which module positions are populated, and what they contain. The elements of this group include

- module number
- module type
- DSP type

To view hardware statistics, follow the procedure below.

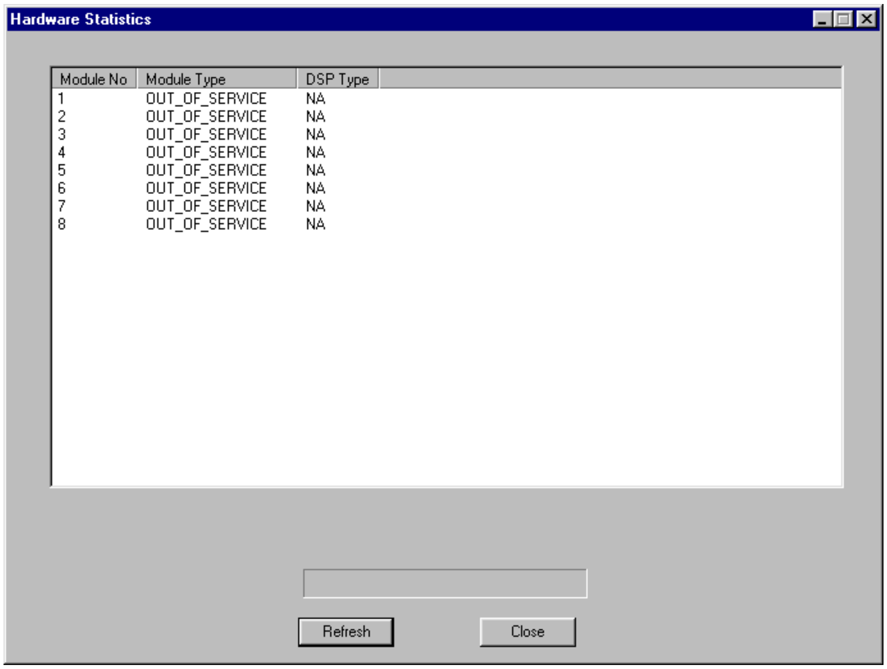
Getting there RLC → Configuration Manager

To display the hardware statistics

1 Choose Alarms/Stats/Logs → Hardware Statistics.

2 Wait while Configuration Manager gathers statistics from the MIG RLC's system logs.

Result: The statistics appear.



Module No	Module Type	DSP Type
1	OUT_OF_SERVICE	NA
2	OUT_OF_SERVICE	NA
3	OUT_OF_SERVICE	NA
4	OUT_OF_SERVICE	NA
5	OUT_OF_SERVICE	NA
6	OUT_OF_SERVICE	NA
7	OUT_OF_SERVICE	NA
8	OUT_OF_SERVICE	NA

3 Do one of the following options:

- To refresh the statistics, click Refresh.
- To close the statistics window, click Close.

Hardware Statistics field descriptions

Column	Description
Module No.	Identifies a module number and, thus, position on the MIG RLC’s motherboard.
Module Type	Identifies what has been installed in the module position: ■ DSP: a DSP application module is installed ■ OUT_OF_SERVICE: no hardware is installed
DSP Type	Identifies the DSP algorithm used by the module.

Section D: Performing upgrades

In this section

Overview

Introduction

This section describes how to perform firmware and software upgrades. Perform firmware upgrades when you have determined that your current firmware or software version is out-of-date.

You can obtain the latest upgrade from the Nortel Networks web site.

Types of upgrades

There are two types of upgrades that can be performed for your MIG RLC:

- a Configuration Manager software upgrade on your PC
- a MIG RLC firmware upgrade

You use the Configuration Manager software to configure or administer the MIG RLC. The firmware contains the code necessary for operating the MIG RLC.

Firmware upgrades

You perform firmware upgrades over the IP network using the software upload option in Configuration Manager. You must have a TFTP server application running on the administration PC. The TFTP server's base directory must point to the directory that contains the upgrade files.

You must ensure that the MIG RLC's firmware has been upgraded before the firmware on Remote Office 9150 units is upgraded. This ensures that communication problems between the MIG RLC and Remote Office 9150 units do not occur.

Software upgrades

The Configuration Manager software upgrade is initiated by running SETUP.EXE.

Verifying the firmware and software version

Introduction

This section describes how to determine the version of firmware and software currently installed.

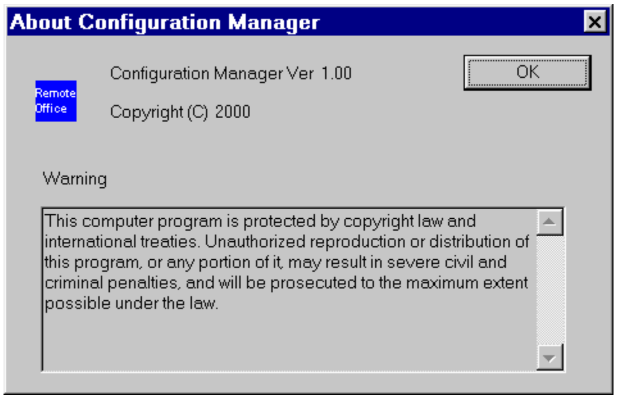
Why verify the firmware and software release

Before you perform a firmware or software upgrade, you should determine what version is currently installed. This ensures that you do not replace the installed firmware or software with an older version.

To verify the software version

From the menu, choose Help → About Configuration Manager.

Result: The following dialog box appears:



About Configuration Manager

Configuration Manager Ver 1.00

Copyright (C) 2000

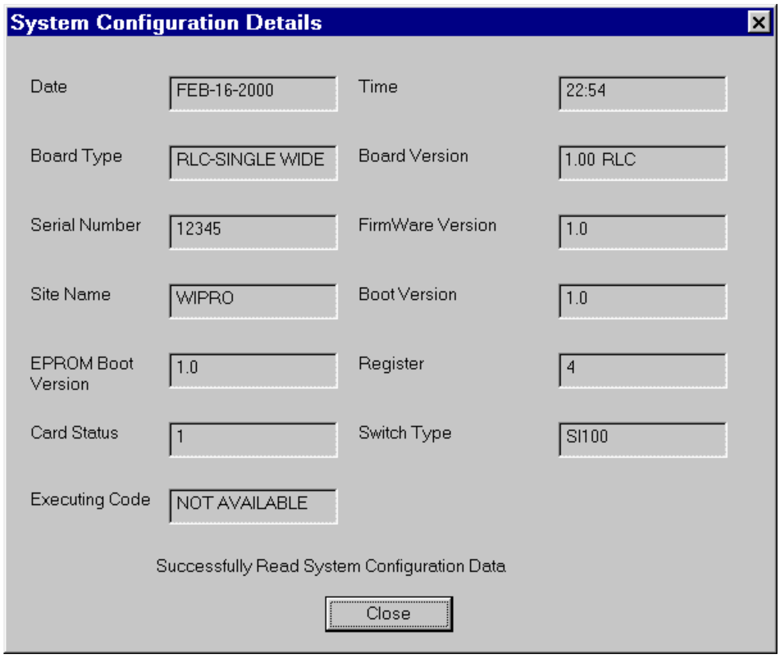
Warning

This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

To verify the firmware version

1 From the menu, choose System Information → System Data.

2 The System Configuration Details screen appears.



System Configuration Details

Date	FEB-16-2000	Time	22:54
Board Type	RLC-SINGLE WIDE	Board Version	1.00 RLC
Serial Number	12345	FirmWare Version	1.0
Site Name	WIPRO	Boot Version	1.0
EPROM Boot Version	1.0	Register	4
Card Status	1	Switch Type	SI100
Executing Code	NOT AVAILABLE		

Successfully Read System Configuration Data

3 Review the Firmware Version box. This identifies the version of firmware installed on the unit.

To determine the current firmware and software versions

To determine the current firmware and software versions, refer to the *Remote Office and MIG RLC Release Notes* (NTP 555-8421-102).

Obtaining the latest upgrade file

Introduction

If you need to upgrade the firmware or software, you can obtain the latest upgrade files from the Nortel Networks web site at http://www.nortelnetworks.com/remoteoffice.

Upgrade files are provided in self-extracting executable files. You must extract the upgrade files before you can perform the upgrade.

Types of upgrades

There are two types of upgrades that can be performed for your MIG RLC:

- Configuration Manager software upgrade

  You use Configuration Manager software to configure or administer the MIG RLC.
- firmware upgrade for the MIG RLC motherboard

  The firmware contains the code necessary for operating the MIG RLC.

  Note: This includes any firmware updates that have been made for DSP application modules.

To download the upgrade file

1. With your web browser, connect to the Nortel Networks web site at http://www.nortelnetworks.com/remoteoffice.
2. Locate the software and firmware you need.
3. Download the files into a temporary location on your PC.
4. Extract the files into a temporary location on your PC by double-clicking the .exe file.
5. Continue with “Extracting upgrade files from the download file” on page 244.

Extracting upgrade files from the download file

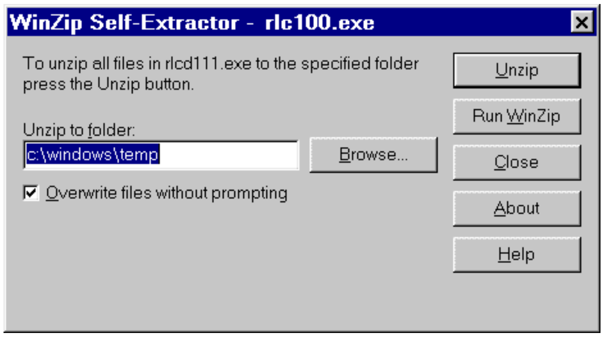
Introduction

Before you perform an upgrade, ensure you have obtained the latest upgrade files from your Nortel Networks distributor. The upgrade files are enclosed in self-extracting executable files. You must extract the upgrade files before you can perform the upgrade.

To perform the extraction using Windows

1. Use Windows Explorer to navigate to the directory that contains the .exe file you received from Nortel Networks.
2. Locate and double-click the .exe file.

   Result: The WinZip Self-Extractor screen similar to the following opens.



WinZip Self-Extractor - rlc100.exe

To unzip all files in rlcd111.exe to the specified folder press the Unzip button.

Unzip to folder: c:\windows\temp

☑ Overwrite files without prompting

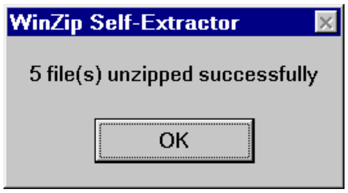
3. Review the information presented and make changes as necessary.

   Notes:

   - It is recommended that you extract the files into a temporary directory.
   - If you specify a directory that does not exist, the WinZip Self-Extractor creates it.

4 Click Unzip.

Result: The file extraction begins. A status bar shows the extraction progress. When completed, a message similar to the following appears:



5 file(s) unzipped successfully

5 Click OK.

Result: The WinZip Self-Extractor screen reappears.

6 Click Close.

Performing a firmware upgrade

Introduction

This section describes how to perform a firmware upgrade on your MIG RLC. You perform the upgrade over the IP network using the TFTP protocol.

You must have a TFTP server application running on the administration PC. The TFTP server's base directory must point to the directory that contains the upgrade files.

When to perform a firmware upgrade

Perform a firmware upgrade if you have determined that you are using out-of-date firmware. For instructions on determining if you need to perform an upgrade, see "Verifying the firmware and software version" on page 241.

CAUTION

Risk of incorrect operation

You must ensure that the MIG RLC's firmware has been upgraded before the firmware on Remote Office 9150 units is upgraded. This ensures that communication problems between the MIG RLC and Remote Office 9150 units do not occur.

About firmware upgrades and configuration files

Each time you perform a firmware upgrade, the configuration database is also converted (if necessary) to a format that is compatible with the new firmware. Configuration settings are not affected by the conversion.

Nortel Networks recommends that each time you perform a firmware upgrade, your first step should be to create a backup copy of the converted configuration file, and store it in a safe secure location.

Before you begin

1 Obtain the firmware upgrade from Nortel Networks.

For instructions, see “Obtaining the latest upgrade file” on page 243.

2 Extract the upgrade files from the file you received from Nortel Networks.

For instructions, see “Extracting upgrade files from the download file” on page 244.

3 Start the TFTP server application.

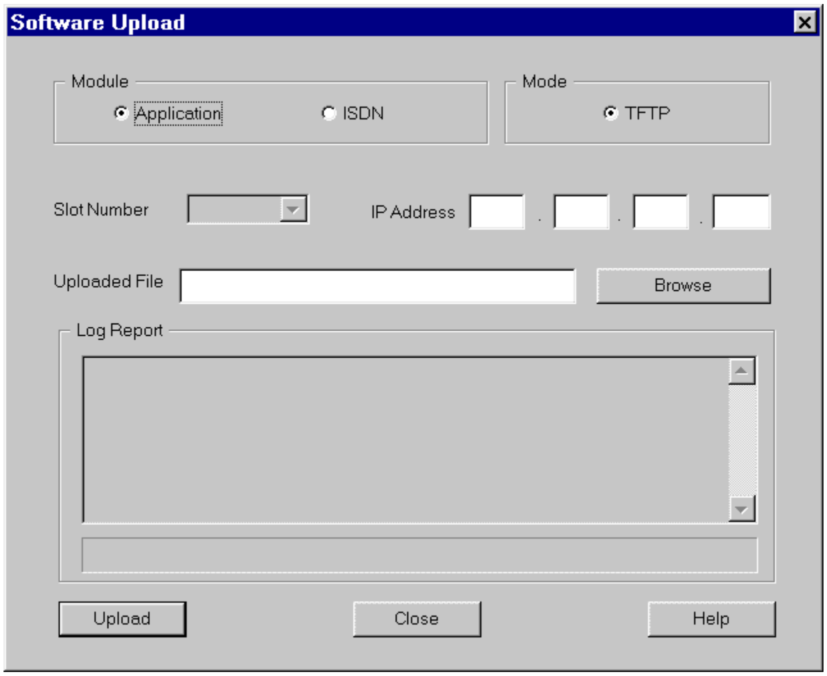
4 Ensure the TFTP base directory reflects the directory where the firmware upgrade file you want to use is located.

Getting there RLC → Configuration Manager

To upgrade Configuration Manager software

1 From the menu, choose Upload/Download → Upload S/W.

Result: The Software Upload screen appears.



Software Upload

Module: ● Application ○ ISDN

Mode: ● TFTP

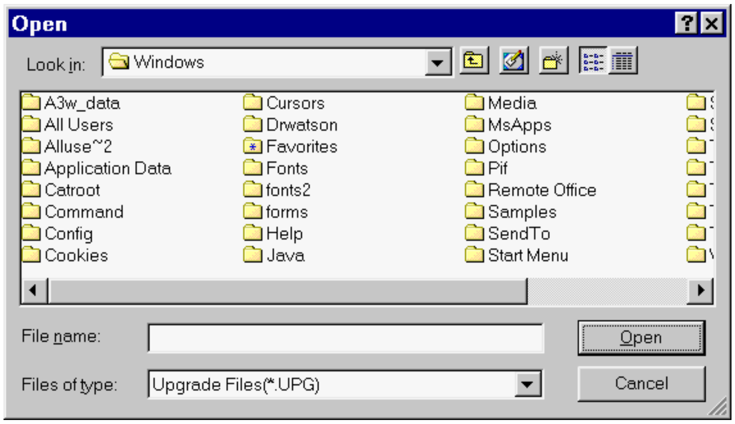
2 In the Module section, click Application.

3 Enter the IP address of the TFTP server into the IP Address boxes.

Note: Since the TFTP server application is running on your administration PC, this is the IP address of the PC.

4 Click Browse.

Result: The Open dialog box appears.



Look in: Windows

File name:

Files of type: Upgrade Files(*.UPG)

5 Ensure the “Files of type” box shows Upgrade Files(*.UPG).

6 Navigate to the folder where the firmware file is located.

7 Select the file, and then click Open.

Example: Select rlc-100.upg, and then click Open.

Result: You return to the Software Upload dialog box. The file you selected is shown in the Uploaded File box.

8 Click Upload.

Wait until the file uploads completely before entering any other commands. The Log Report box displays a confirmation message when the upgrade is completed.

9 Restart the MIG RLC.

Performing a software upgrade

Introduction

Perform a software upgrade if you have determined that you are using out-of-date software. For instructions on determining if you need to perform an upgrade, see “Verifying the firmware and software version” on page 241.

To upgrade the Configuration Manager software

1. Use Windows Explorer to navigate to the directory that contains the upgrade files you extracted.
2. Locate and double-click the setup.exe file.
3. Follow the prompts on the screen.

ATTENTION Do not ignore any warning messages that the InstallShield displays about versions of files (such as DLL files) that already exist on your PC. If you overwrite these files, you can inadvertently cause other applications on your PC to stop working.

Result: The InstallShield installs the software on top of the previous version.

Chapter 8

Troubleshooting

In this chapter

Overview

Introduction

If you experience problems in setting up or running your MIG RLC, this chapter helps you to isolate and solve the problem.

Before you begin

The questions listed on page 253 can help you determine the proper course of action for addressing your specific problem.

Meridian Internet Gateway Reach Line Card LEDs

The primary purpose of MIG RLC LEDs is to give you an indication of the line card's general health. See the section beginning on page 254 for descriptions of proper LED behavior and responses to improper behavior.

Connectivity

The section beginning on page 256 has procedures for checking connectivity at the host and remote sites, identifying some problems that can occur on the data network, and resolving those problems.

Software problems

If you have trouble completing a task with Configuration Manager, see pages 260 and 261 for help in determining what to do.

Before you begin

Introduction

The questions listed in this section can help you determine the proper course of action for addressing your problem.

Identifying why a problem occurred

Before you begin, ask yourself the questions listed in the following table:

Question	IF you answered	THEN do the following
Is this a new installation?	yes	Perform the troubleshooting in the sequence presented in this chapter.
	no	Answer the next question.
Did the MIG RLC work, and then suddenly stop working?	yes	Answer the next question.
	no	Perform troubleshooting in the sequence presented in this chapter.
Did you modify the configuration or change any hardware components?	yes	**1** Verify that changes were made correctly. **2** Check the hardware components to ensure they are working correctly. **3** Perform troubleshooting for the specific component in which the problem appears.
	no	Contact your telecom or data network administrator. There might be a problem with the network.

Meridian Internet Gateway Reach Line Card LEDs

Introduction

The primary purpose of MIG RLC LEDs is to give you an indication of the line card's general health. When you reset your MIG RLC, watch the faceplate. The LEDs should behave as follows:

- The Maintenance LED should flash three times, and then go off after the switch enables the MIG RLC. (In normal operation of the MIG RLC, the Maintenance LED should remain off.)
- The remaining LEDs flash whenever there is network activity.

What to do if the LEDs do not display correctly

The following table describes what to do if the LEDs do not display correctly:

Symptom	What to do
The Maintenance LED did not flash three times during the power-up cycle.	**1** Reset the MIG RLC. Watch the Maintenance LED again. About 60 seconds pass before it flashes. **2** If the Maintenance LED still does not flash, contact your Nortel Networks distributor. There might be a hardware problem.
The Maintenance LED is lit after a successful self-test.	**1** Check to see if the slot is enabled on the PBX. **2** If other LEDs are not lit or flashing, did the Maintenance LED *ever* light? If not, contact your Nortel Networks distributor. There might be a hardware problem. **3** Ensure that the MIG RLC is properly seated in its slot and is properly inserted into the backplane.

Symptom	What to do
The Maintenance LED is lit after a successful self-test. (continued)	**4** If the card is improperly or incompletely seated, reseat it. If the Maintenance LED remains lit, contact your Nortel Networks distributor. There might be a hardware problem.
The Maintenance LED is flashing.	The power-up self-test failed. Contact your Nortel Networks distributor. There might be a hardware problem.
No LEDs are lit on the MIG RLC.	Ensure that the MIG RLC is properly seated in its slot. If the MIG RLC is properly seated in its slot and no LEDs light, contact your Nortel Networks distributor. There might be a hardware problem.
The Ethernet COLL LED is lit solid.	Network collisions are bound to occur and are normal. However, if this LED is lit solid, do the following: **1** Check the physical network connection. **2** Verify that the MIG RLC can be pinged. **3** Check the network configuration (such as routing, traffic load, and so on). Adjust the network configuration, if required. **4** There should be no broadcast or multicast activity on the telephony LAN (TLAN). Interconnect a hub and a network analyzer to the TLAN and monitor for such activity. Identify the source(s) and isolate them from the TLAN.

Connectivity

Introduction

This section describes problems that can occur on the network and what to do to resolve those problems.

Symptom descriptions

If you are not able to establish or maintain data network connectivity, perform troubleshooting as described in the following table:

Symptom	What to do
You cannot establish a connection from your administration PC to the MIG RLC.	**1** Ensure that you entered the IP address correctly when trying to establish the connection. **2** Ensure that you entered the logon ID and password correctly when trying to establish the connection. **3** Ensure the MIG RLC's IP address, network mask, and default gateway are correctly configured in the MIG RLC. **4** Ping the MIG RLC. **5** Ping the gateway. **6** If the ping still does not work, contact your data network administrator.
`10060 TELNET CONNECTION FAILED` appears when attempting to connect to the MIG RLC.	**1** Ensure that you entered the logon ID and password correctly when trying to establish the connection. **2** Ensure that you entered the IP address correctly when trying to establish the connection. **3** Ensure someone is not already logged on to the MIG RLC.

Symptom	What to do
10060 TELNET CONNECTION FAILED appears when attempting to connect to the MIG RLC. (continued)	**4** Verify that the Ethernet cable is connected at both ends (MIG RLC and network hub). **5** Check the Ethernet cable and ensure it is good. **6** Ensure the MIG RLC is properly seated in its slot. **7** Verify that the IP address, subnet mask, and gateway are all correct on the MIG RLC. **8** Ping the MIG RLC. **9** If the MIG RLC does not respond, ping the MIG RLC's gateway to see if it responds. **10** If the gateway does not respond, ping a known good device on the MIG RLC's network. **11** If steps 9 and 10 work, but step 8 did not, there may be a gateway configuration error. Check the unit's IP Configuration property sheet. **12** Contact your Nortel Networks distributor. There might be a hardware problem.
SERIAL CONNECTION FAILED appears when attempting to connect to the MIG RLC.	**1** Ensure that you entered the logon ID and password correctly when trying to establish the connection. **2** Ensure that someone is not already logged on to the MIG RLC. **3** Ensure the MIG RLC is properly seated in its slot. **4** Reseat the MIG RLC. **5** Ensure you specified the correct COM port when attempting the connection. **6** Verify that no other applications on the administration PC are using the COM port.

Symptom	What to do
`SERIAL CONNECTION FAILED` appears when attempting to connect to the MIG RLC. (continued)	**7** Check the serial cable connection to ensure it is good. **8** Use a breakout box to verify that the COM port is active. **9** Contact your Nortel Networks distributor. There might be a hardware problem.
The MIG RLC will not send or receive Ethernet traffic.	**1** Ensure the MIG RLC is seated in its slot properly and connected to the backplane. **2** Check the Ethernet cable between the MIG RLC and the network, and ensure that it is good. **3** Ensure the Ethernet cable is connected. **4** If the MIG RLC still will not send or receive traffic, contact your data network administrator. **5** Data network administrator: Ensure other network devices are configured to allow traffic to and from the MIG RLC.
An attempt to log off from the MIG RLC does not work.	It is possible that communication has been lost between the administration PC and the MIG RLC. Close Configuration Manager, and then restart it.
There are many collisions on the Ethernet network, as indicated by the solid Ethernet COLL LED.	Network collisions are bound to occur and are normal. However, if this LED is lit solid, do the following: **1** Check the physical network connection. **2** Verify that the MIG RLC can be pinged. **3** Check the network configuration (such as routing, traffic load, and so on). Adjust the network configuration, if required.

Symptom	What to do
There are many collisions on the Ethernet network, as indicated by the solid Ethernet COLL LED. (continued)	**4** There should be no broadcast or multicast activity on the TLAN. Interconnect a hub and a network analyzer to the TLAN and monitor for such activity. Identify the source(s) and isolate them from the TLAN.
The MIG RLC cannot establish a connection with the Remote Office 9150 unit.	**1** Verify security authentication configuration and ensure that it matches at both ends. (For example, if the security identifier security level is used, ensure that the inbound and outbound security identifiers are correctly configured at each end.) **2** Ensure that the unit IDs have been correctly configured at each end. An incorrect unit ID causes security authentication to fail. **3** Ensure that the MIG RLC's IP address and PSTN number are correctly configured on the Remote Office 9150 unit (and vice versa). **4** Verify that the IP and circuit-switched networks are operational (up and running) as appropriate. **5** Ensure that the MIG RLC is enabled on the host PBX. **6** Use the Ping option in Configuration Manager to ping the remote unit. For instructions, see "To perform a Configuration Manager ping" on page 262. **7** If the remote unit does not respond, check the network configuration (such as, routing, traffic load, and so on). Adjust the network configuration, if required.

Software problems

Introduction

This section identifies some problems that can occur with the Configuration Manager software, and describes what to do to resolve them.

Symptom descriptions

If you are not able to complete a task with Configuration Manager, perform troubleshooting as described in the following table:

Symptom	What to do
The Configuration Manager software installation fails.	Ensure that you close all background applications, including anti-virus checking software before performing the installation.
When performing one of the following by TFTP, `ERROR: FILE OPEN FAILED` appears: ■ configuration upload ■ MIG RLC firmware upgrade	**1** Ensure the TFTP server application is installed and running on your administration PC. **2** Ensure the file you are trying to upload is present in the target directory. That is, either in the TFTP directory, or in the directory that is specified as the base directory in the TFTP server application. **3** Review messages displayed by the TFTP server application for clues. **4** Ping the MIG RLC to verify that network connectivity exists.
`CONFIG UPLOAD FAILED` when attempting to perform a configuration upload by TFTP.	**1** Ensure that you selected an appropriate file. That is, ensure that the file you attempted to upload is a MIG RLC configuration file.

Symptom	What to do
`CONFIG UPLOAD FAILED` when attempting to perform a configuration upload by TFTP. (continued)	**2** Ensure that the configuration file you are attempting to upload is compatible with current MIG RLC firmware. Perform the configuration upload using a previous configuration file, if necessary. **Note:** Each time you perform a MIG RLC firmware upgrade, you should also create a backup of the configuration. The configuration database format in the MIG RLC is dependent on the version of firmware installed on the MIG RLC. If you recently downgraded to a previous version of MIG RLC firmware, you might also need to revert to a previous configuration format.
`System not responding` appears when working with Configuration Manager.	It is possible that communication has been lost between the administration PC and the MIG RLC. Close Configuration Manager, and then restart it.
Nothing happens when attempting to log off from the MIG RLC.	It is possible that communication has been lost between the administration PC and the node to which you were logged on. Close Configuration Manager, and then restart it.

Using Configuration Manager’s Ping

Introduction

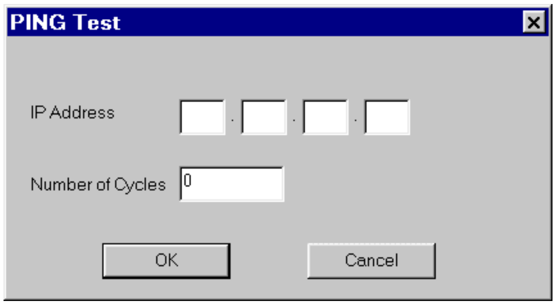
This section explains how to use the Ping option provided in Configuration Manager to verify connectivity. Use this procedure as a troubleshooting tool to determine if you can reach the Remote Office 9150 unit, another MIG RLC, or any other device on the network.

Getting there RLC → Configuration Manager

To perform a Configuration Manager ping

1 From the menu, choose Tests → Ping.

Result: The PING Test dialog box appears.



PING Test

IP Address □ . □ . □ . □

Number of Cycles 0

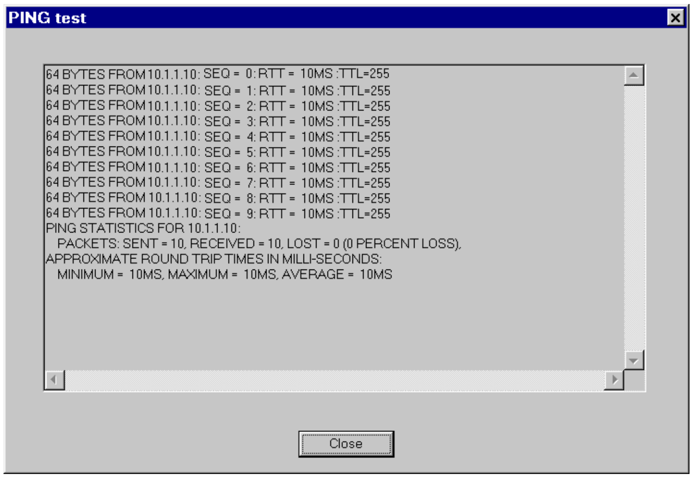
2 Enter the IP Address of the unit you want to ping.

3 In the Number of Cycles box, enter the number of times you want to ping the unit.

The number must be in the range of 1–100.

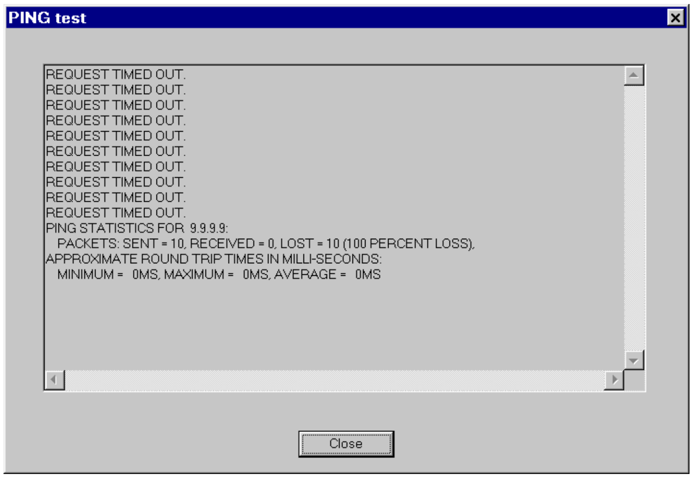
4 Click OK.

Result: The PING test results screen appears, showing the ping results. The following is an example of a successful ping:



```
64 BYTES FROM 10.1.1.10: SEQ =  0: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  1: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  2: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  3: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  4: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  5: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  6: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  7: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  8: RTT =  10MS :TTL=255
64 BYTES FROM 10.1.1.10: SEQ =  9: RTT =  10MS :TTL=255
PING STATISTICS FOR 10.1.1.10:
   PACKETS: SENT = 10, RECEIVED = 10, LOST = 0 (0 PERCENT LOSS),
APPROXIMATE ROUND TRIP TIMES IN MILLI-SECONDS:
   MINIMUM =  10MS, MAXIMUM =  10MS, AVERAGE =  10MS
```

The following is an example of an unsuccessful ping:



```
REQUEST TIMED OUT.
REQUEST TIMED OUT.
REQUEST TIMED OUT.
REQUEST TIMED OUT.
REQUEST TIMED OUT.
REQUEST TIMED OUT.
REQUEST TIMED OUT.
REQUEST TIMED OUT.
REQUEST TIMED OUT.
REQUEST TIMED OUT.
PING STATISTICS FOR  9.9.9.9:
   PACKETS: SENT = 10, RECEIVED = 0, LOST = 10 (100 PERCENT LOSS),
APPROXIMATE ROUND TRIP TIMES IN MILLI-SECONDS:
   MINIMUM =   0MS, MAXIMUM =   0MS, AVERAGE =   0MS
```

5 Click Close.

Result: The Ping test screen closes.

ATTENTION

It is possible to successfully ping a device on the network and still not be able to log on to that device. If you log on to a device (for example, the MIG RLC) via serial connection and neglect to log off, you can successfully ping the device but cannot establish a Telnet connection to it. (The device believes itself to be busy.)

If you cannot log on to a device after a successful ping, go to the serial port and ensure that you are not logged on to the device via this port.

What to do if the ping did not work

1. Did you enter the IP address correctly?
2. Are the subnet mask and default gateway configured properly at your site? (Confirm this by checking the IP Configuration property sheets for the involved units.)
3. Are the subnet mask and default gateway configured properly at the site that you are pinging? (Confirm with the site's network administrator.)
4. Does the gateway respond to a ping?

If you answer "Yes" to the questions above and the ping still does not work, the problem lies somewhere in the network between the involved sites.

Responding to a catastrophic failure

Introduction

For the purposes of this discussion, a *catastrophic failure* is defined as a failure of the equipment to operate.

Inoperative hardware

Should your MIG RLC fail to operate, consult your Nortel Networks distributor for hardware replacement.

Appendix A

Network engineering guidelines

In this appendix

Overview

Introduction

Traditionally, Meridian 1 networks depended on voice services such as LEC and IXC private lines.

Note: For the sake of abbreviation, the term “voice services” also includes fax services.

With Remote Office technology, the Meridian 1 can select a new delivery mechanism, one that uses packet-switching over a data network or corporate intranet. The role of the Remote Office node is to convert steady-stream digital voice into fixed-length IP packets. The IP packets are transported across the IP data network with a low latency that varies with strict limits.

History

In the data world in the late 1960s, IP evolved from a protocol that allowed multi-vendor hosts to communicate. The protocol adopted packet switching technology, providing bandwidth efficiency for bursty data traffic that can tolerate high latency and jitter (variation in latency). Since IP supported the TCP transport layer, which provided connection-oriented and reliable transport, IP took on the properties of being connectionless and a best-effort delivery mechanism.

Present day

Now, there are new considerations when the same corporate network is expected to deliver voice traffic. The intranet introduces impairments, delay, delay variation, and data packet loss, at levels that are higher than those delivered by voice networks. Delay between talker and listener changes the dynamics and reduces the efficiency of conversations, while delay variation and packet errors cause glitches in conversation.

Connection of the Remote Office nodes to the corporate intranet without preliminary assessments can result in unacceptable degradation in the voice service. Instead, you must consider correct design procedures and principles.

Understanding your network

A good design of the Remote Office network must begin with an understanding of traffic, and the underlying network that transmits the traffic. You must do the following preliminary tasks:

1. Calculate Remote Office traffic.

   You must estimate the amount of traffic that the Meridian 1 system will route through the Remote Office network. This, in turn, places a traffic load on the corporate intranet. This is described in “Remote Office traffic engineering” on page 271.

2. Assess wide area network (WAN) link resources.

   If resources in the corporate intranet are not enough to adequately support voice services, it is normally caused by not enough WAN resources. “Assessing WAN link resources” on page 282 outlines how you can make this check.

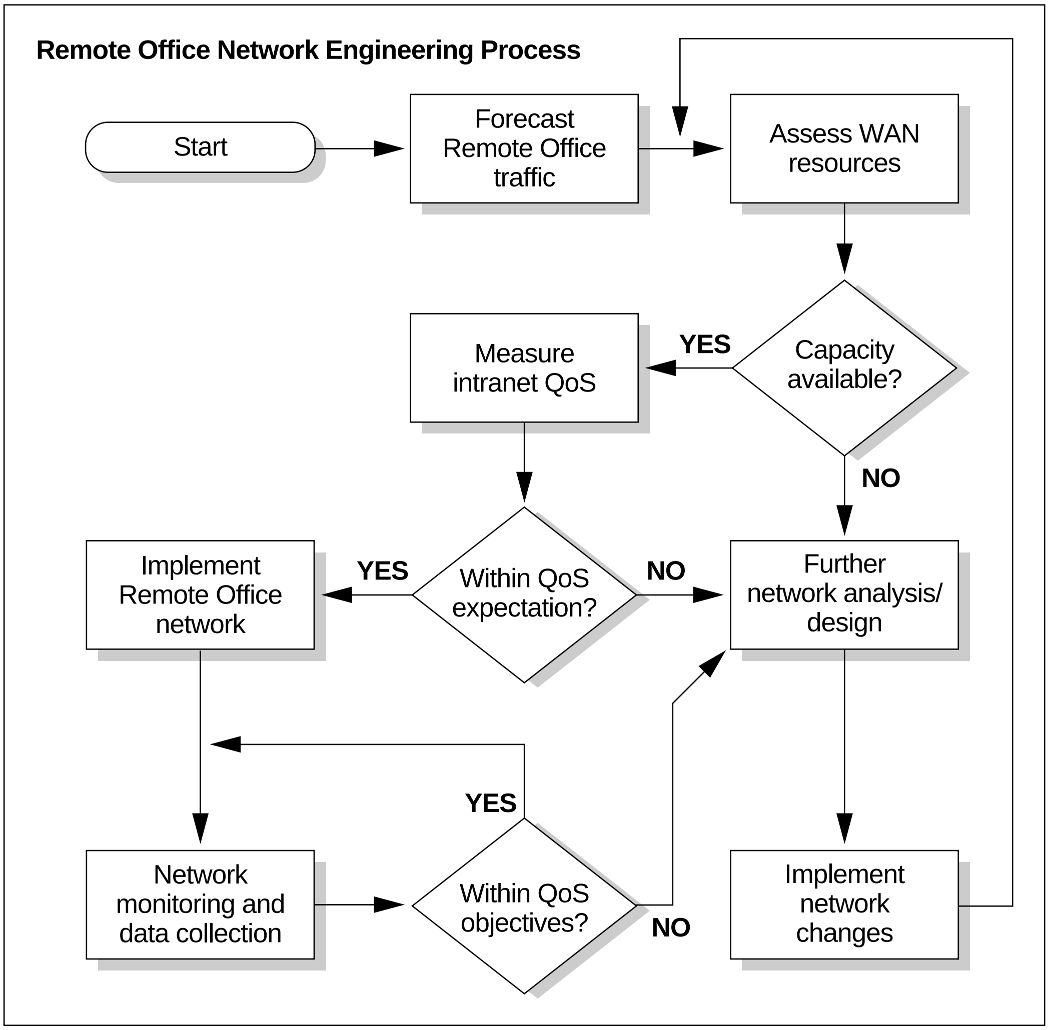
3. Measure the existing intranet’s QoS.

   You must estimate the quality of voice service the corporate intranet can deliver. “Measuring the intranet Quality of Service” on page 299 describes how to measure the prevailing delay and error characteristics of an intranet.

After the assessment phase, you can design and implement the Remote Office network. This design not only involves the Remote Office elements, but can also require making design changes to your intranet. “Fine-tuning the network Quality of Service” on page 304 and “Implementing Quality of Service in IP networks” on page 312 provides guidelines for making modifications to the intranet.

The following flowchart shows the design and planning decisions that should take place.

Remote Office network engineering flowchart


Remote Office Network Engineering Process
Start
Forecast Remote Office traffic
Assess WAN resources
Capacity available?
YES
Measure intranet QoS
NO
Within QoS expectation?
YES
Implement Remote Office network
NO
Further network analysis/ design
YES
Network monitoring and data collection
Within QoS objectives?
NO
Implement network changes

G101421

Remote Office traffic engineering

Introduction

To design a network, you must size it so that it can accept some calculated amount of traffic. The purpose of the Remote Office network is to deliver voice traffic meeting the QoS objectives. Since traffic determines network design, the design process needs to start with determining a Remote Office traffic forecast. The traffic forecast drives

- WAN requirements
- Remote Office hardware requirements
- telephony local area network (TLAN) requirements

Ethernet and WAN bandwidth

The table on page 272 lists the Ethernet and WAN bandwidth use of Remote Office ports with different codecs. One port is a channel fully loaded to 36 centi-call-seconds (CCS), where one CCS is a channel or circuit being occupied for 100 seconds. 36 CCS is a circuit occupied for a full hour.

To calculate the bandwidth requirement of a route, divide the total route traffic by 36 CCS and multiply by the bandwidth use to get the data rate requirement of that route. All traffic data must be based on the busy hour of the busy day.

To calculate resource requirements (Remote Office ports and TLAN or WAN bandwidth), traffic parcels are summarized in different ways:

1. Add together all sources of traffic for the Remote Office network (for example, voice, faxes sent, and faxes received), to calculate Remote Office port and TLAN requirements.
2. For data rate requirements at each route, base the calculation on each destination pair.
3. For fax traffic on a WAN, account for only the larger of either the fax-sent or fax-received traffic.

The engineering procedures for TLAN and WAN are different. The following calculation procedure is for TLAN. The modification required for WAN engineering is included.

A WAN route with a bandwidth of 1.536 Mbps or more can be loaded up to 80% (voice packets must have priority over data). A smaller WAN pipe (64 Kbps) is recommended to a loading of 50%.

When the WAN route prioritizes VoIP traffic over data traffic, the route bandwidth can be engineered to a 90% loading level. Otherwise, it can be engineered to an 80% loading level.

TLAN Ethernet and WAN IP bandwidth usage per Remote Office port

The following table identifies TLAN Ethernet and WAN IP bandwidth usage per Remote Office port.

Notes:

- The first WAN bandwidth is without Frame Relay or ATM overhead.
- The Frame Relay overhead is eight bytes (over IP packet).
- The Link Layer Control SubNetwork Attachment Point (LLC SNAP) and AAL5 overhead for ATM is 16 bytes (over IP packet).
- IP packet size over 53 bytes requires two ATM cells, IP packet size over 106 bytes requires three ATM cells, and so on. Within the same number of cells, the bandwidth requirements are the same for packets with different sizes.

	Codec type			
Bandwidth usage	**G.711 (64 Kbps)**	**G.726 (32 Kbps)**	**G.729AB G.729A (8 Kbps)**	**T.38 G3 Fax modem (14.4 Kbps)**
Codec Multi-frame duration in ms (payload) (one way)	30	30	30	25
Voice/fax payload Multi-frame in bytes (one way)	240	120	30	30

	Codec type			
Bandwidth usage	**G.711 (64 Kbps)**	**G.726 (32 Kbps)**	**G.729AB G.729A (8 Kbps)**	**T.38 G3 Fax modem (14.4 Kbps)**
IP voice packet in bytes (one way)	280	160	70	70
Ethernet voice packet in bytes (one way)	306	186	96	96
Bandwidth use on TLAN in Kbps (two way)	97.9	85.3	30.7	30.7
Bandwidth use on WAN in Kbps (one way)	44.8	42.7	11.2	22.4
WAN with Frame Relay overhead in Kbps (one way)	46.1	44	12.5	25.0
WAN with ATM overhead in Kbps (one way)	59.4	57.3	17.0	33.9

Notes:

1. TLAN data rate is the effective Ethernet bandwidth consumption.
2. TLAN Kbps for voice traffic = (1-40%)*2*Ethernet frame bytes*8/frame duration in ms
3. WAN Kbps for voice traffic = (1-40%)*IP packet bytes*8/frame duration in ms
4. Overhead of (RTP + UDP + IP) packets over the voice payload multiframe is 40 bytes. Overhead of Ethernet frame over IP packet is 26 bytes.
5. The bandwidth calculation does not include an Interframe gap because of the low probability of it occurring in this type of application.

To calculate TLAN traffic

1 Calculate Voice on IP Traffic

CCS/user=# of calls/set * Average Holding Time (in seconds)/100

Total voice CCS (Tv) = CCS/user*No. of VoIP users

The number of VoIP users (phonesets) is the potential population in the system that can generate/receive traffic through the Remote Office node. You can estimate this number.

Base the VoIP traffic on measured route traffic from traffic report TFC002, which provides CCS for each route.

2 Calculate fax on IP Traffic

CCS/user sending fax = # of pages sent/fax * Average Time to send a page (default 48 seconds)/100

CCS/user receiving fax = # of pages received/fax * Average Time to receive a page (default 48 seconds)/100

Total fax CCS (Tx) = CCS/fax sent*No. of users sending fax + CCS/fax received* No. of users receiving fax

The user who sends or receives a fax can be the same person or different persons. It is the number of faxed documents and the average number of pages per faxed document that are important. The time unit for fax traffic is also the busy hour. The busy hour selected must be the hour that gives the highest combined voice and fax traffic.

3 Calculate the total Remote Office CCS

Total Remote Office traffic (T) = Tv + Tx

4 Calculate the bandwidth output. Refer to the table shown on page 272. Tv/36 and Tx/36 indicate the average number of simultaneous callers.

Note: This calculation requires perfectly queued and perfectly smooth traffic.

Tv/36*bandwidth output per port = voice bandwidth per node (Bv)

Tx/36*bandwidth output per port = fax bandwidth per node (Bx)

Total bandwidth (Bt) = Bv + Bx

For WAN calculation, you only need to consider the larger of fax traffic sent or received.

5 Adjust requirement for traffic peaking

Peak hour bandwidth per node = Bt*1.3 (default)

A peak factor of 1.3 is the default value used to account for traffic fluctuation in the busy hour due to non-queued, Poisson random distribution of call originations.

Example: Remote Office ports and TLAN engineering

The procedure shown here is for the Remote Office port and TLAN data requirement calculation. In the WAN environment, the traffic parcel is defined per destination pair (route). The total node traffic should be subdivided into destination pair traffic. The rest of the calculation procedure continues to be applicable.

A configuration with 120 VoIP users each generates 4 calls using IP network (originating and terminating) with an average holding time of 150 seconds in the busy hour.

In the same hour, 25 faxes are sent and 20 faxes are received. The faxes sent average 3 pages, while the faxes received average 5 pages. The average time to set up and complete a fax page delivery is 48 seconds.

The preferred codec is G.729 Annex AB, and the voice packet payload is 30 ms. The fax modem speed is 14.4 Kbps, and the payload is 16.6 ms. How many Remote Office ports are needed? What is the traffic in Kbps generated by this node to TLAN?

1 Calculate Voice on IP Traffic during busy hour

CCS/user = 4*150/100 = 6 CCS

Tv = 120*6 = 720 CCS

2 Calculate fax on IP Traffic during busy hour

CCS/fax sent = 3*48/100 = 1.44 CCS

CCS/fax received = 5*48/100 = 2.4 CCS

Total fax CCS (Tx + Rx) = 1.44*25 + 2.4*20 = 36+ 48 = 84 CCS

3 Remote Office Traffic during busy hour

Total traffic (T) = Tv + Tx = 720 + 84 = 804 CCS

4 Calculate average bandwidth use on TLAN

For voice:

720/36*30.7 = 614 Kbps

According to the table on page 272, the data output for G.729 Annex AB and 30 ms payload is 30.7 Kbps.

For fax:

84/36*46.1 =108 Kbps

Total bandwidth = 614 + 108 = 722 Kbps

5 Adjust requirement for traffic peaking

Peak hour bandwidth requirement = 722*1.3 = 939 Kbps

This is the spare bandwidth that a TLAN should have to handle the VoIP and fax traffic. Nortel Networks recommends that the TLAN handle Remote Office traffic exclusively.

Note: This example is based on the G.729 Annex AB codec with 30 ms payload size. For relations of user selectable parameters (for example, payload size, codec type, packet size and QoS), refer to "Setting the Quality of Service" on page 294.

General LAN and WAN engineering considerations

The TLAN traffic capacity does not limit Remote Office network engineering. Refer to standard Ethernet engineering tables for passive 10BaseT repeater hubs. Refer to manufacturer's specifications for intelligent 10BaseT layer switches.

A passive 10BaseT Ethernet hub is a half-duplex data transport mechanism. Both "talk" and "listen" traffic use a part of the nominal 10 Mbps capacity. You must set up the passive 10BaseT Ethernet hub so that TLAN voice traffic does not exceed 3 Mbps on a 10BaseT Ethernet. A 10BaseT Ethernet switch port can operate in either half-duplex or full-duplex mode, but Remote Office Ethernet interfaces operate only in half-duplex mode. A switched Ethernet hub can reach throughput of 10 Mbps. For more information, refer to your manufacturer's specifications.

Due to its high capacity, 100BaseT Ethernet does not experience bottlenecks.

WAN links are normally based on PSTN standards such as DS0, DS1, DS3, SONET STS-3c, or Frame Relay. These standards are full-duplex communication channels.

With standard PCM encoding (G.711 codec), a two-way conversation channel has a rate of 128 Kbps (that is, 64 Kbps in each direction). The same conversation on WAN (for example ISDN PRI) requires a 64 Kbps channel only, because a WAN channel is a full duplex channel.

When Remote Office nodes share a segment of Ethernet in the simplex mode, the average loading on Ethernet should not exceed 30%.

When simplex/duplex Ethernet links terminate on the ports of an Ethernet switch (for example, Baystack 450), the fully duplex Ethernet up-link to the router/WAN can be loaded to 60% on each direction of the link.

A WAN route with a bandwidth of 1.536 Mbps or more can be loaded up to 80% (voice packets must have priority over data). A single DS0 WAN pipe (64 Kbps) is recommended to a loading of 50%.

When the WAN route prioritizes VoIP traffic over data traffic, the route bandwidth can be engineered to a 90% loading level. Otherwise, it can be engineered to an 80% loading level.

Fax engineering considerations

Fax calculation is based on a 30 byte packet size and a data rate of 64 Kbps (no compression). The frame duration (payload) is calculated by using the equation 30*8/14400=16.6 ms, where 14 400 bps is the modem data rate. Bandwidth output is calculated by the equation 108*8*1000/16.6=52.0 Kbps. Bandwidth output to WAN is 70*8*1000/16.6 = 33.7 Kbps.

Payload and bandwidth output for other packet sizes or modem data rates must go through similar calculations.

Fax traffic is always one-way. Fax pages sent and fax pages received generate data traffic to the TLAN. For WAN calculation, you only need to consider the larger traffic parcel of the two.

WAN route engineering

After TLAN traffic is calculated, determine the bandwidth requirement for the WAN. In this environment, bandwidth calculation is based on network topology and destination pair.

Before network engineering can begin, you must collect the following network data:

- Obtain a network topology and routing diagram.
- List the sites where the Remote Office nodes are to be installed.
- List the site pairs with Remote Office traffic, and the codec and frame duration (payload) to be used.
- Obtain the offered traffic in CCS for each site pair. If available, separate voice traffic from fax traffic (fax traffic sent and received).
- In a network with multiple time zones, use the same real-time busy hour (varying clock hours) at each site that yields the highest overall network traffic.
- Traffic to a route is the sum of voice traffic plus the larger of one way fax traffic (either sent or received).

To illustrate this process, see the following multi-node engineering example.

Traffic flow of a 4-node Remote Office network

Destination pair	Traffic in CCS
Santa Clara/Richardson	60
Santa Clara/Ottawa	45
Santa Clara/Tokyo	15
Richardson/Ottawa	35
Richardson/Tokyo	20
Ottawa/Tokyo	18

The codec selection is based on a per Remote Office unit basis. During call setup negotiation, only the type of codec available at both destinations is selected. When no agreeable codec is available at both ends, the default codec G.711 is used.

Note: Nortel Networks recommends that all units in a Remote Office system have the same image. If multiple codec images are used in a Remote Office network, the calls default to the G.711 group when the originating and destination codecs are different.

Determining MIG RLC requirements

The Remote Office port requirement for each node is calculated by counting the traffic on a per node basis. See the table in “Incremental WAN bandwidth requirements” below.

The port requirements are shown in the following table:

Remote Office site	Traffic in CCS	Remote Office ports	Number of MIG RLCs
Santa Clara	120	9	1
Richardson	115	9	1
Ottawa	98	8	1
Tokyo	53	6	1

This assumes that the preferred codec to handle VoIP calls in this network is G.729 Annex AB.

Incremental WAN bandwidth requirements

The table on the next page summarizes the WAN traffic in Kbps for each route. Note that the recommended incremental bandwidth requirement is included in the column adjusted for 30% traffic peaking in busy hour.

This assumes no correlation and no synchronization of voice bursts in different simultaneous calls.

Destination pair	CCS on WAN	WAN traffic in Kbps	Peaked WAN traffic (x 1.3) in Kbps
Santa Clara/Richardson	60	18.7	24.3
Santa Clara/Ottawa	45	14.0	18.2
Santa Clara/Tokyo	15	4.7	6.1
Richardson/Ottawa	35	10.9	14.2
Richardson/Tokyo	20	6.2	8.1
Ottawa/Tokyo	18	5.6	7.3

Calculating the bandwidth requirement

The following example illustrates the calculation procedure for Santa Clara and Richardson.

- The total traffic on this route is 60 CCS.
- To use the preferred codec of G.729 Annex AB with 30 ms payload, the bandwidth use on the WAN is 11.2 Kbps. (See “TLAN Ethernet and WAN IP bandwidth usage per Remote Office port” on page 272.)
- Calculate WAN traffic using the following formula:

  (60/36)*11.2 = 18.7 Kbps
- Augment this number by 30% to calculate the peak traffic rate: 24.3 Kbps.

  This is the incremental bandwidth required between Santa Clara and Richardson to carry the 60 CCS voice traffic during the busy hour.

Assume that 20 CCS of the 60 CCS between Santa Clara and Richardson is fax traffic. Of the 20 CCS, 14 CCS is from Santa Clara to Richardson, and 6 CCS is from Richardson to Santa Clara. What is the WAN data rate required between those two locations?

Traffic between the two sites can be broken down to 54 CCS from Santa Clara to Richardson, and 46 CCS from Richardson to Santa Clara, with the voice traffic 40 CCS (=60-20) being the two-way traffic.

The bandwidth requirement calculation is

(40/36)*11.2 + (14/36)*33.6 = 25.51 Kbps

where 14 CCS is the larger of two fax traffic parcels (14 CCS as compared to 6 CCS).

After adjusting for peaking, the incremental data rate on WAN for this route is 33.2 Kbps. Compare this number with 24.3 Kbps when all 60 CCS is voice traffic. It appears that the reduction in CCS due to one-way fax traffic (20 CCS as compared to 14 CCS) will not compensate for higher bandwidth requirement of a fax, as compared to voice traffic (33.7 Kbps as compared to 11.2 Kbps).

Assessing WAN link resources

Introduction

For most installations, Remote Office traffic is routed over WAN links within the intranet. WAN links are the most expensive repeating expenses in the network, and they often are the source of capacity problems in the network. Unlike LAN bandwidth, which is virtually free and easily implemented, WAN links, especially inter-LATA and international links, take time to obtain financial approval, provision, and upgrade. For these reasons, it is important to determine the state of WAN links in the intranet before installing the Remote Office network.

Each voice conversation (G.729 Annex AB codec, 30 ms payload) consumes 11.2 Kbps of bandwidth or 18.6 Kbps for *each* link that it traverses in the intranet. A DS0 64 Kbps WAN link supports five simultaneous telephone conversations.

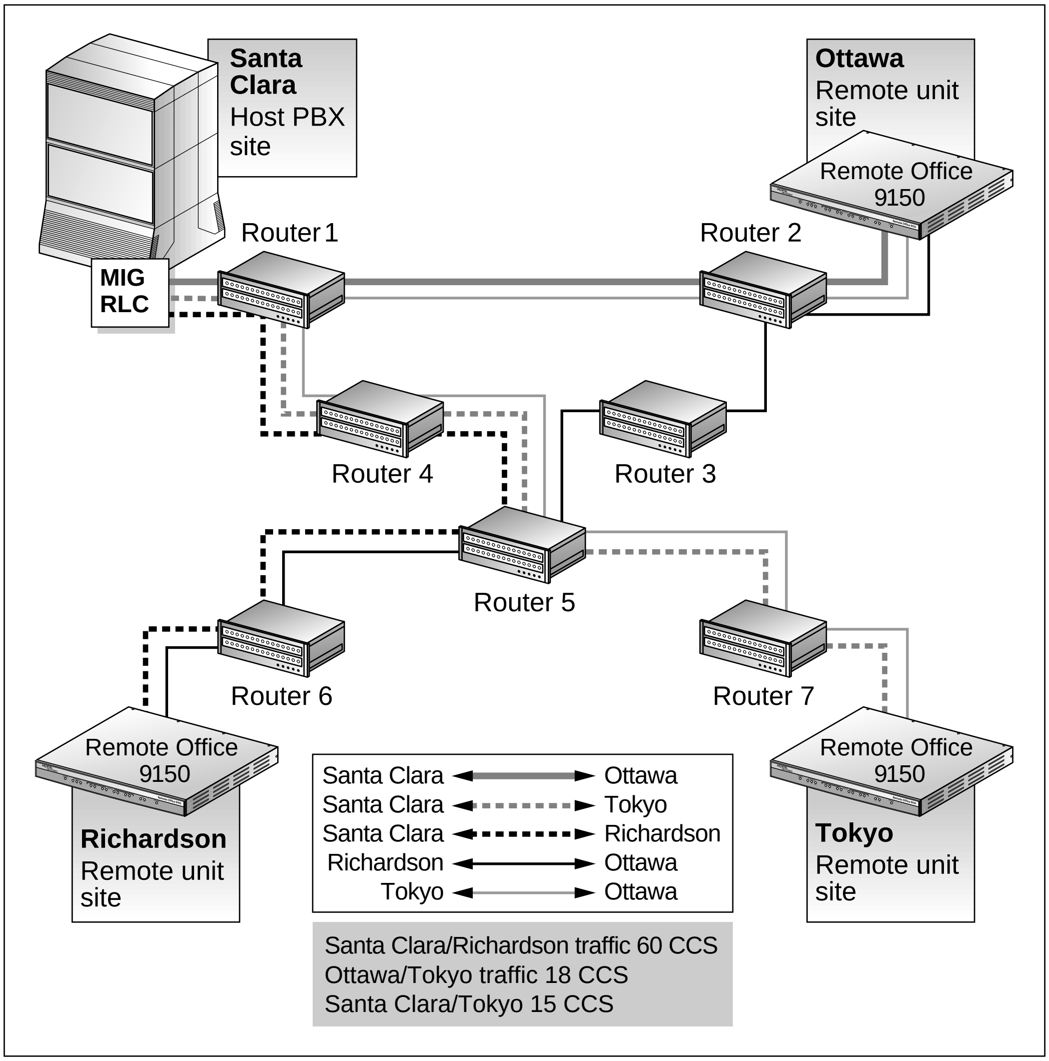
Determining the state of WAN links

1 Obtain a current topology map and link utilization report of the intranet.

A visual inspection of the topology map should reveal which WAN links are likely to be used to deliver Remote Office traffic.

Note: For an example, see the network topology map on page 283. Alternatively, use the traceroute tool. See “Measuring the intranet Quality of Service” on page 299.

Network topology map



G101422

2 Determine the current link utilization.

Note the reporting window that appears in the link utilization report. For example, the link utilization can be averaged over a week, a day, or one hour.

To be consistent with the dimensioning considerations (see “Remote Office traffic engineering” on page 271), obtain the busy period (for example, peak hour) utilization of the trunk.

Also, because WAN links are full-duplex and data services exhibit asymmetric traffic behavior, obtain the utilization of the link representing traffic flowing in the heavier direction.

3 Determine how much spare capacity is available.

Enterprise intranets are subject to capacity planning policies that ensure that capacity use remains below some determined utilization level. For example, a planning policy might state that the utilization of a 56 Kbps link during the peak hour must not exceed 50%. For a T1 link, the threshold is higher, say 80%.

The carrying capacity of the 56 Kbps link is 28 Kbps, and for the T1 1.2288 Mbps. In some organizations, the thresholds can be lower than that used in this example.

Spare capacity must be available to reroute traffic when link failures occur.

Some WAN links can actually be provisioned on top of layer 2 services, such as Frame Relay and ATM. The router-to-router link is actually a virtual circuit, which is subject to not only a physical capacity, but also a “logical capacity” limit. You must obtain, in addition to the physical link capacity, the QoS parameters. The important QoS parameters are committed information rate (CIR) for Frame Relay, and maximum cell rate (MCR) for ATM.

The difference between the current capacity and its allowable limit is the available capacity. For example, a T1 link utilized at 48% during the peak hour, with a planning limit of 80% has an available capacity of about 492 Kbps.

Estimating network loading caused by Remote Office traffic

At this point, you have enough information to “load” the Remote Office traffic on the intranet. The “Network topology map” on page 283 illustrates how this is done on an individual link.

Suppose you want to predict the amount of traffic on the Router 4-Router 5 link. From the “Remote Office traffic engineering” section and traceroute measurements, the Router 4-Router 5 link is expected to support the Santa Clara/ Richardson, Santa Clara/Tokyo, and Ottawa/Tokyo traffic flows. The other Remote Office traffic flows do not route over the Router 4-Router 5 link. The summation of the three flows yields 93 CCS or 24 Kbps as the incremental traffic that the Router 4-Router 5 link needs to support.

To complete this exercise, calculate the traffic flow from every site pair to calculate the load on each link.

Determining the route links

You must record routing information for all source-destination pairs as part of the network assessment. You can do this by using the traceroute tool. An example of the output is shown below:

```
Richardson3 % traceroute santa_clara_Remote Office4
traceroute to santa_clara_Remote Office4 (10.3.2.7), 30
hops max, 32 byte packets
Router 6 (10.8.0.1) 1 ms  1 ms  1 ms
Router 5 (10.18.0.2) 42 ms  44 ms  38 ms
Router 4 (10.28.0.3) 78 ms  70 ms  81 ms
Router 1 (10.3.0.1) 92 ms  90 ms  101 ms
santa_clara_Remote Office4 (10.3.2.7) 94 ms  97 ms  95
ms
```

You can use the traceroute program to check if routing in the intranet is symmetric for each of the source-destination pairs. Use the `-g` loose source routing option, as shown in the following command syntax:

```
Richardson3 % traceroute -g santa_clara_Remote Office4
richardson3
```

Note: The option letter can be different depending on vendor implementation.

The traceroute program identifies the intranet links that transmit Remote Office traffic. For example, if the traceroute of four site pairs yields the results shown in the following table, then the load of Remote Office traffic per link can be calculated as shown in the "Route link used for each site pair" table that follows.

Site pair	Intranet route
Santa Clara/Richardson	Router 1-Router 4-Router 5-Router 6
Santa Clara/Ottawa	Router 1-Router 2
Santa Clara/Tokyo	Router 1-Router 4-Router 5-Router 7
Richardson/Ottawa	Router 2-Router 3-Router 5-Router 6

Route link used for each site pair

This link	Routes traffic between
Router 1-Router 2	Santa Clara and Ottawa Tokyo and Ottawa
Router 1-Router 4	Santa Clara and Richardson Santa Clara and Tokyo Ottawa and Tokyo
Router 2-Router 3	Richardson and Ottawa
Router 3-Router 5	Richardson and Ottawa
Router 4-Router 5	Santa Clara and Richardson Santa Clara/Tokyo Ottawa and Tokyo
Router 5-Router 6	Santa Clara and Richardson Richardson and Ottawa
Router 5-Router 7	Santa Clara and Tokyo Ottawa and Tokyo

Determining if there is enough capacity

The following table arranges the calculations so that for each link, the available link capacity can be compared against the additional Remote Office load. For example, on the link between Router 4 and Router 5, there is plenty of available capacity (492 Kbps) to accommodate the additional 24 Kbps of Remote Office traffic.

	End points		
Link capacity	**Router 1 and Router 2**	**Router 1 and Router 4**	**Router 4 and Router 5**
Capacity (Kbps)	1536	1536	1536
Utilization %			
■ Threshold	80	80	80
■ Used	75	50	48
Available capacity (Kbps)	76.8	460.8	492
Incremental Remote Office load—site pair	Santa Clara/Ottawa Ottawa/Tokyo	Santa Clara/Tokyo Santa Clara/ Richardson Ottawa /Tokyo	Santa Clara/ Richardson Ottawa/Tokyo Santa Clara/Tokyo
Incremental Remote Office load—traffic (Kbps)	21.2	31.4	31.4

Some network management systems have network planning modules that compute network flows in the manner just described. These modules provide more detailed and accurate analysis as they can take into account actual node, link, and routing information. They also help you assess network resilience by conducting link and node failure analysis. By simulating failures, and reloading network and recalculated routes, the modules indicate where the network might be out of capacity during failures.

What to do if there is insufficient link capacity

If there is not enough link capacity, upgrade the link’s bandwidth.

Other intranet resource considerations

Bottlenecks caused by non-WAN resources are less frequent. For a more complete assessment, you must consider the impact of incremental Remote Office traffic on routers and LAN resources in the intranet. Perhaps the Remote Office traffic will traverse LAN segments that are saturated, or routers whose CPU utilization is high.

Quality of Service evaluation process overview

Introduction

There are two main objectives when dealing with the QoS issue in a Remote Office network:

- to predict the expected QoS
- to evaluate the QoS after integrating Remote Office traffic into the intranet

The process for either case is similar. One case is without Remote Office traffic. The other case is with Remote Office traffic.

To evaluate the Quality of Service

It is assumed that the ping command is available on a Windows PC, or that a network management tool provides the ability to collect delay and loss data.

1. Use ping or an equivalent tool to collect round-trip delay (in ms) and loss (in %) data.
2. Divide the delay by 2 to approximate one-way delay, and add 93 ms to adjust for Remote Office processing and buffering time.
3. Refer to the “Quality of Service levels” table on page 290 to predict the QoS categories (excellent, good, fair, or poor).
4. If you want to manage the QoS in a more detailed fashion, you can rebalance the values of delay compared to loss by adjusting Remote Office system parameters, such as preferred codec, payload size, routing algorithm, and so on, to move resulting QoS among different categories.
5. If the QoS objective is met, repeat the process periodically to make sure the required QoS is maintained.

Quality of Service levels

You can use the following table to estimate the IP telephony QoS level based on QoS measurements of the intranet. To limit the size of this table, the packet loss and one-way delay values are tabulated in increments of 1% and 10 ms respectively. The techniques used to determine and apply the information in this table are Nortel Networks proprietary.

Note: The QoS levels are equivalent to the following Mean Opinion Score (MOS) values:

- excellent: 5
- good: 4
- fair: 3
- poor: 2

		Quality of Service level		
Packet loss (%)	**One-way delay (ms)**	**G.729A**	**G.726**	**G.711A or G.711u**
0	50-200	excellent	excellent	excellent
0	210-220	excellent	excellent	excellent
0	230-330	good	excellent	excellent
0	340-360	good	good	good
0	370-380	good	good	good
0	390-620	fair	good	good
0	630-780	fair	fair	fair
0	790	fair	fair	fair
1	50-180	excellent	excellent	excellent
1	190-200	good	good	excellent
1	210-320	good	good	good

		Quality of Service level		
Packet loss (%)	One-way delay (ms)	G.729A	G.726	G.711A or G.711u
1	330-340	good	good	good
1	350-360	fair	good	good
1	370-630	fair	fair	fair
1	640-690	fair	fair	fair
1	700-780	poor	fair	fair
2	50-270	good	good	good
2	280-300	good	good	good
2	310-320	good	fair	fair
2	330-510	fair	fair	fair
2	520-580	fair	fair	fair
3	50-250	good	good	good
3	260	good	good	good
3	270-460	fair	fair	fair
3	470-490	fair	fair	fair
4	50-200	good	good	good
4	210-240	good	good	good
4	250-390	fair	fair	fair
4	400-440	fair	fair	fair
5	50-180	good	good	good
5	190-210	good	good	good

		Quality of Service level		
Packet loss (%)	One-way delay (ms)	G.729A	G.726	G.711A or G.711u
5	220-360	fair	fair	fair
5	370-400	fair	fair	fair
6	50-200	good	good	good
6	210-330	fair	fair	fair
6	340-380	fair	fair	fair
7	50-140	good	good	good
7	150-310	fair	fair	fair
7	320-340	fair	fair	fair
8	50-290	fair	fair	fair
8	300-320	fair	fair	fair
9	50-270	fair	fair	fair
9	280-300	fair	fair	fair
10	50-260	fair	fair	fair
10	270-280	fair	fair	fair
11	50-250	fair	fair	fair
11	260-270	fair	fair	fair
12	50-230	fair	fair	fair
12	240-260	fair	fair	fair
13	50-230	fair	fair	fair
13	240-250	fair	fair	fair

		Quality of Service level		
Packet loss (%)	**One-way delay (ms)**	**G.729A**	**G.726**	**G.711A or G.711u**
14	50-210	fair	fair	fair
14	220-230	fair	fair	fair
15	50-190	fair	fair	fair
15	200-230	fair	fair	fair
16	50-160	fair	fair	fair
16	170-210	fair	fair	fair

Setting the Quality of Service

Introduction

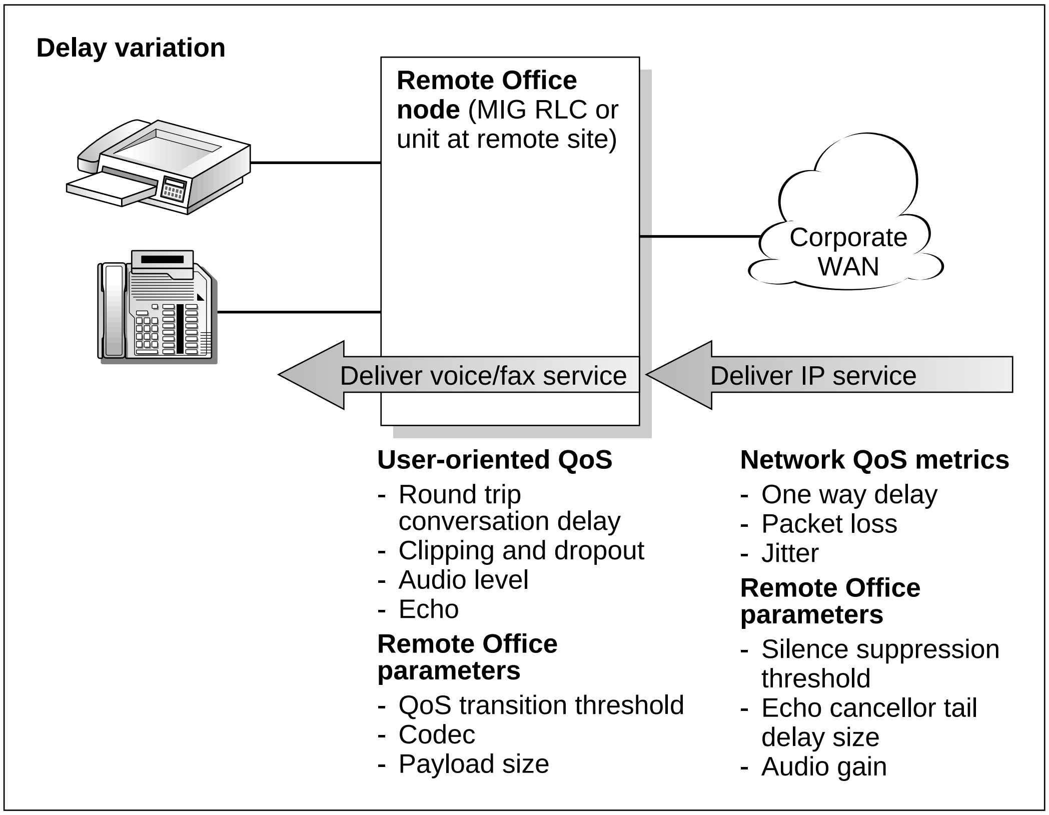
The users of corporate voice and data services expect these services to meet some perceived QoS, which, in turn, influences network design. The goal is to design and allocate enough resources in the network to meet the users' needs. QoS metrics or parameters are what quantify the needs of the service user.

Relationship between users and services

In the context of a Meridian 1 and Remote Office system, the diagram on page 295 shows the relationship between users and services.

From the diagram, you can see that there are two interfaces that you must consider:

- The Remote Office node (that is, the MIG RLC on the PBX or the Remote Office unit at a remote site) interfaces with the end users. Voice services offered by the Remote Office node must meet user-oriented QoS objectives.
- The Remote Office nodes interface with the intranet. The service provided by the intranet is "best-effort delivery of IP packets," not "guarantee QoS for real-time voice transport." The Remote Office node translates the QoS objectives set by the end-users into IP-oriented QoS objectives. The guidelines call these objectives *intranet QoS objectives*.



G101423

The Remote Office node monitors the intranet's QoS. The *transition threshold* parameter on the Remote Office node then dictates the minimum *QoS level* of the Remote Office network. Note that the transition threshold is set on a per site-pair basis.

The *QoS level* is a user-oriented QoS metric and takes on one of ten settings, which indicates the quality of voice service. Remote Office periodically calculates the prevailing QoS level per site-pair based on its measurement of

- one-way delay
- packet loss
- codec

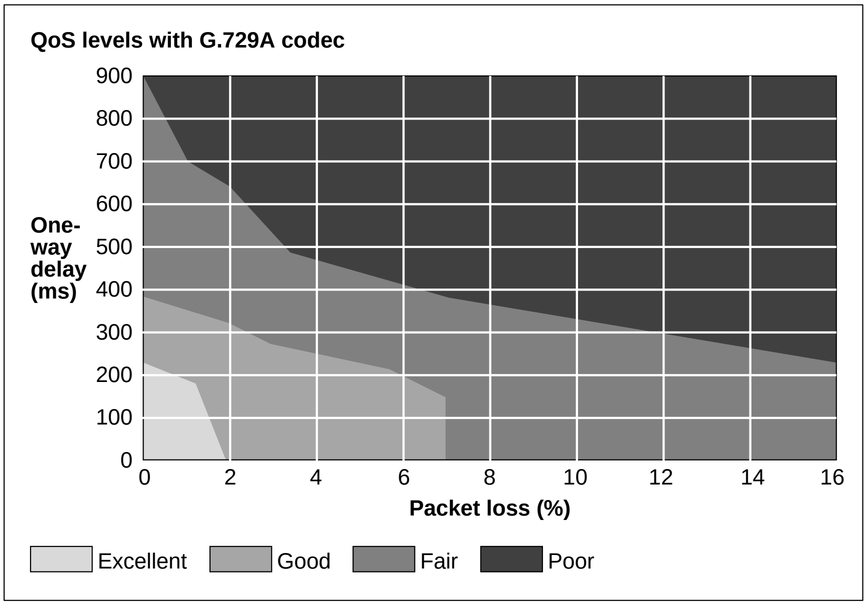
When the QoS level is below the transition threshold, calls to that destination are rerouted over circuit-switched voice facilities. When QoS returns to a point above the set threshold, calls are restored to the IP network.

The calculation is derived from the E-model in ITU-T Reg. G.114 and on ANSI TR56. When the QoS level falls below the transition threshold levels for that particular destination, that call is not accepted by the originating Remote Office node. Instead, the call is rerouted by the host PBX features over traditional circuit-switched voice facilities.

Quality of Service levels by codec

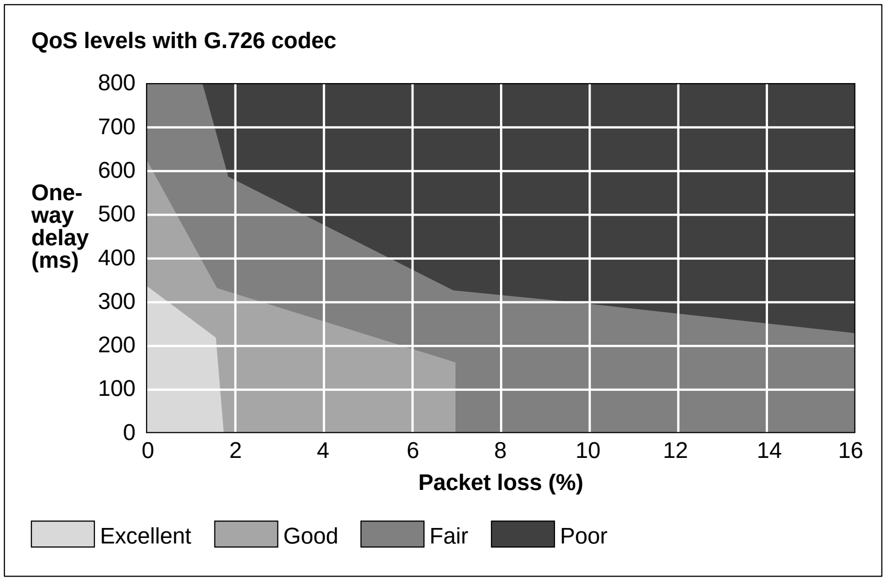
The QoS level graphs on pages 297 and 298 show the operating regions in terms of *one-way delay* and *packet loss* for each codec and required QoS level as determined by Remote Office. Note that among the codecs, G.711(A-law) and G.711(u-law) deliver the best quality for a given intranet QoS, followed by G.729A. These graphs determine the delay and error budget for the underlying intranet in order for it to deliver a required quality of voice service.

Fax is more susceptible to packet loss than the human ear. Quality starts to degrade when packet loss exceeds 10%. Nortel Networks recommends that fax services be supported with the Remote Office operating in either the Excellent or Good QoS level. Avoid offering fax services between site pairs that can guarantee no better than a Fair or Poor QoS level.



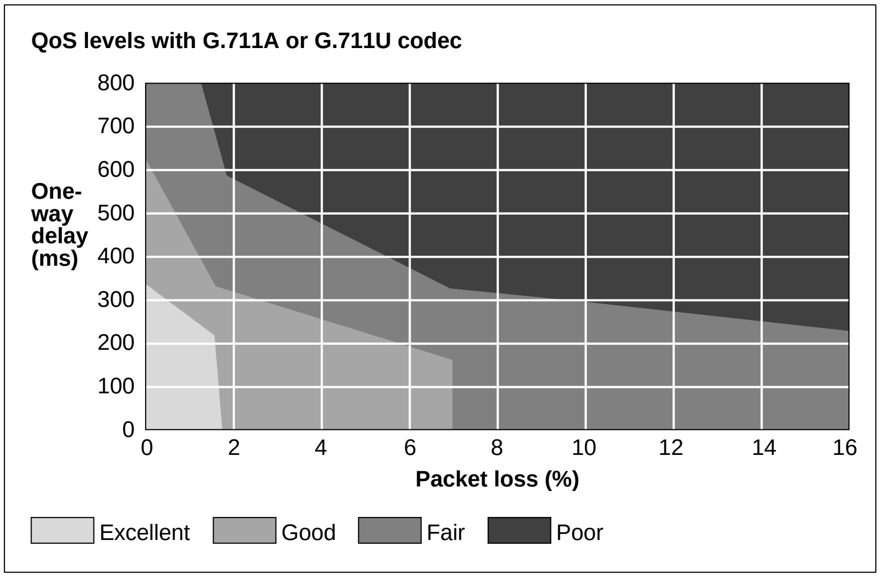
QoS levels with G.729A codec

G101424



QoS levels with G.726 codec

G101425


QoS levels with G.711A or G.711U codec
One-way delay (ms)
800
700
600
500
400
300
200
100
0
0
2
4
6
8
10
12
14
16
Packet loss (%)
Excellent
Good
Fair
Poor

G101425

Measuring the intranet Quality of Service

Introduction

You can measure end-to-end delay and error characteristics of the current state of the intranet. These measurements help you set acceptable QoS standards when using the corporate intranet to transmit voice services.

Measuring end-to-end network delay

The basic tool used in IP networks to measure end-to-end network delay is the ping command. Ping takes a delay sample by sending an ICMP packet from the host of the ping command to a destination server. Ping then waits for the packet to make a round trip. The ping output is similar to the following:

```
Richardson3 % ping -s santa_clara_Remote Office4 60
PING santa_clara4 (10.3.2.7): 60 data bytes
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=97ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=100ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=102ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=97ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=95ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=94ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=112ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=97ms
^?
--- Richardson3 PING Statistics ---
8 packets transmitted, 8 packets received, 0% packet
loss round-trip (ms) min/avg/max = 94/96/112
```

The time field displays the round trip time (*rtt*).

In order for the delay sample results to match what the Remote Office node can experience, the ping host must be on a working LAN segment attached to the router intended to support the Remote Office node. The selection of destination host is just as important, following these same guidelines for the source host.

The size of the ping probe packets must be set to 60 bytes to approximate the size of probe packets sent by the Remote Office node that are used in determining when new calls need to transition to the circuit-switched network.

Notice the variation of *rtt* from the ping output. You can obtain a delay characteristic of the intranet from repeated sampling of *rtt*. In order to obtain a delay distribution, the ping tool can be embedded in a script that controls the frequency of the ping probes, and timestamps and stores the samples in a raw data file. The file can then be analyzed later using spreadsheet and other statistics packages. You can check if the intranet's network management software has any delay measurement modules that can obtain a delay distribution for specific site pairs.

Delay characteristics vary depending on the site pair and the time of day. The assessment of the intranet should include taking delay measurements for each Remote Office site pair. If there are significant fluctuations of traffic in the intranet, it is best to include ping samples during the intranet's peak hour. For a more complete assessment of the intranet's delay characteristics, obtain ping measurements over a period of at least a week.

Measuring end-to-end packet loss

The ping program also reports if the ICMP packet made its round trip correctly. In fact, use the same ping host setup to measure end-to-end error, and, as in making delay measurement, use the same packet size parameter.

Sampling error rate, however, requires taking multiple ping samples (at least 30 to be statistically significant). Thus, obtaining an error distribution requires running ping over a greater period of time. The error rate statistic collected by multiple ping samples is called *packet loss rate* (PLR).

Adjusting ping measurements

One-way as compared to round trip

The ping statistics are based on round trip measurements, whereas the QoS metrics in the Transmission Rating model are one-way. In order to make the comparison compatible, the delay and packet error ping statistics must be halved.

Adjustment caused by Remote Office processing

The ping measurements are taken from ping host to ping host. The Transmission Rating QoS metrics are from end user to end user, and include components outside the intranet. The ping statistic for delay needs to be further modified by adding 93 ms to account for the processing and jitter buffer delay of the Remote Office nodes.

No adjustment needs to be made for error rates.

If the intranet measurement barely meets the round trip QoS objectives, the craftsperson must be aware that there is a possibility that the one-way QoS is not met in one of the flow directions. This can be true even if the flow is on a symmetric route due to the asymmetric behavior of data processing services.

Late packets

Packets that arrive outside of the window allowed by the jitter buffer are discarded by the MIG RLC or Remote Office 9150 unit. To determine which ping samples to ignore, first calculate the average *one-way delay* based on all the samples, and then add 500 ms. This is the maximum delay. All samples whose one-way delay exceed this maximum are considered to be late packets and are removed from the sample. Calculate the percentage of late packets, and add it to the *packet loss* statistic.

Network delay and packet loss evaluation example

From ping data, calculate the average one-way delay (halved from ping output, and adding 93 ms Remote Office processing delay) and standard deviation for latency. Do a similar calculation for packet loss without adjustment.

You add a standard deviation to the mean of both delay and loss for planning purposes. You might want to know whether traffic fluctuation in your intranet reduces the user’s QoS.

Sample measurement results for the G.729A codec

The following table provides a sample measurement of network delay and packet loss for the G.729A codec between various nodes.

	Measured One way delay (ms)		Measured Packet loss (%)		Expected QoS level	
Destination pair	**Mean**	**Mean+σ**	**Mean**	**Mean+σ**	**Mean**	**Mean+σ**
Santa Clara/ Richardson	171	179	1.5	2.1	Excellent	Good
Santa Clara/Ottawa	120	132	1.3	1.6	Excellent	Excellent
Santa Clara/Tokyo	190	210	2.1	2.3	Good	Good
Richardson/Ottawa	220	235	2.4	2.7	Good	Good
Richardson/Tokyo	305	345	2.2	2.6	Good	Fair
Ottawa/ Tokyo	260	286	2.4	2.8	Good	Fair

As an example, the delay and loss pair of traffic from Santa Clara to Richardson (171 ms and 1.5%) meets excellent criterion, but their counterpart with standard deviation (179 ms and 2.1%) can achieve only “good” QoS.

Since the algorithm implemented in Remote Office calculates mean only and not standard deviation, it confirms the “excellent” rating (if the objective is set for excellent, it will not transition to alternate facilities), but you have up to a 50% chance to experience a service level inferior to “excellent” level.

In contrast, the site pair Santa Clara/Ottawa has both QoS levels of mean and mean+σ falling in the excellent region. You have more confidence (better than an 84% chance under the assumption of Normal distribution) that during the peak traffic period, the “excellent” service level is likely to be upheld.

Other measurement considerations

The ping statistics described previously measure the intranet prior to Remote Office installation, which means that the measurement does not take into consideration the expected load offered by the Remote Office users.

If the intranet capacity is tight and the Remote Office traffic is significant, you should consider making intranet measurements under load. Load can be applied using traffic generator tools. The amount of load should match the Remote Office traffic estimated in “Remote Office traffic engineering” on page 271.

Obtaining Quality of Service measurement tools

The ping and traceroute commands are standard IP tools that are usually included with a network host’s TCP/IP stack. You can find a survey of QoS measurement tools and packages (including commercial ones) on the home page of the Cooperative Association for Internet Data Analysis (CAIDA) at http://www.caida.org. Some of these are delay monitoring tools that include features like timestamping, plotting, and computation of standard deviation.

Determining if the intranet meets expected Remote Office Quality of Service

At the end of this measurement and analysis, you should have a good indicator whether the corporate intranet as it stands can deliver adequate voice and fax services. To gauge the QoS level for each site pair, see the “Expected QoS level” column on page 302.

In order to offer voice and fax services over the intranet, you should keep the network within a Good or Excellent QoS level at the Mean+σ operating region. You should not offer fax services on routes that have only Fair or Poor QoS levels.

If the expected QoS levels of some or all routes fall short of being Good, you must evaluate the options and costs for upgrading the intranet. You can estimate the amount of *one-way delay* that must be reduced to raise the QoS level. “Fine-tuning the network Quality of Service” on page 304 provides guidelines for reducing *one-way delay.* Often this involves a link upgrade, a topology change, or implementation of QoS in the network.

You can decide to keep costs down, and accept a temporary Fair QoS level for a selected route. In that case, having made a calculated trade-off in quality, you need to carefully monitor the QoS level, reset expectations with the end users, and be receptive to user feedback.

Fine-tuning the network Quality of Service

Topics presented in this section deal with issues that impact the QoS of Remote Office traffic. They are informative for understanding how to fine-tune a network to improve its QoS, but are not directly involved as a part of network engineering procedure. These are advanced topics to help a technician fine-tune the network to improve QoS, but they are not a part of the required procedure for initial Remote Office network engineering.

Further network analysis

This section describes actions that could be taken to investigate the sources of delay and error in the intranet. This and the next section discuss several strategies for reducing *one-way delay* and *packet loss*. The key strategies are to

- reduce link delay
- reduce hop count
- adjust jitter buffer size
- implement IP QoS mechanisms

Components of delay

End-to-end delay is contributed by many delay components. The major components of delay are

- propagation delay
- serialization delay
- queuing delay
- routing and hop count
- Remote Office system delay
- router processing delay
- LAN segment delay

Propagation delay

Propagation delay is affected by the mileage and medium of links traversed. Within an average size country, the one-way propagation delay over terrestrial lines is under 18 ms. Within the United States, the propagation delay from coast-to-coast is under 40 ms. To estimate the propagation delay of long-haul and transoceanic circuits, use 1 ms per 100 terrestrial miles.

If a circuit goes through a satellite system, estimate each hop between earth stations to contribute 260 ms to the propagation delay.

Serialization delay

This is the time it takes to transmit the voice packet one bit at a time over a WAN link. The serialization delay depends on the voice packet size and the link bandwidth, and is given by the following formula:

Serialization delay in ms = 8*(IP packet size in bytes)/(link bandwidth in Kbps)

The following table shows the serialization delay for voice packets on a 64 Kbps and 128 Kbps link. The serialization delay on higher speed links is considered negligible.

Codec	Frame duration	Serialization delay over 64 Kbps link (ms)	Serialization delay over 128 Kbps link (ms)
G.711A G.711U	10 ms	14.00	0.88
	20 ms	24.00	1.50
	30 ms	34.00	2.13
G.726	30 ms	20	12
G.729A G.729 Annex AB	10 ms	5.25	0.33
	20 ms	6.50	0.41
	30 ms	7.75	0.48

Queuing delay

Queueing delay is the time it takes for a packet to wait in the transmission queue of the link before it is serialized. On a link where packets are processed in first-come-first-serve order, the average queueing time in ms is estimated by the formula

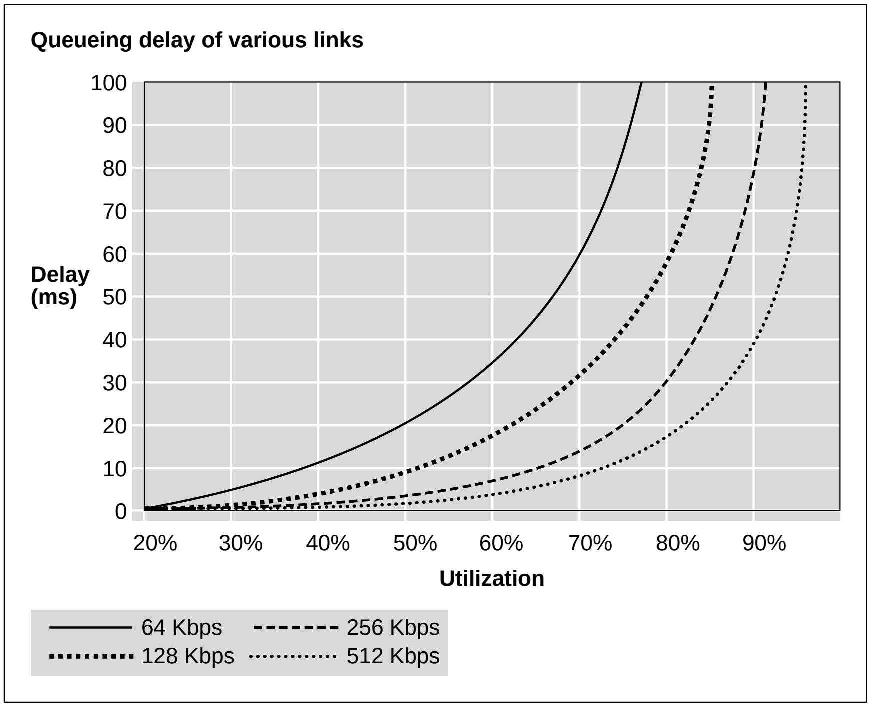
p*p*(average intranet packet in bytes)/(1-p)/(link speed in Kbps),

where p is the link utilization level.

The average size of intranet packets carried over WAN links generally lies between 250 and 500 bytes.

Queuing delay of various links

The diagram on page 306 displays the average queueing delay of the network based on a 300-byte average packet size.



G101426

As you can see, queueing delays can be significant for links with bandwidth under 512 Kbps, whereas with higher speed links, they can tolerate much higher utilization levels.

Routing and hop count

Each site pair takes different routes over the intranet. The route taken determines the number and type of delay components that add to end-to-end delay. Sound routing in the network depends on correct network design at many levels, such as the architecture, topology, routing configuration, link, and speed.

Remote Office system delay

The transmitting and receiving of Remote Office nodes together contribute a processing delay of about 33 ms to end-to-end delay. This is the amount of time required for the encoder to analyze and packetize speech, and by the decoder to reconstruct and depacketize the voice packets.

There is a second component of delay that occurs on the receiving Remote Office node. For every call terminating on the receiver, there is a jitter buffer that serves as a holding queue for voice packets arriving at the destination Remote Office. The purpose of the jitter buffer is to smooth out the effects of delay variation so that a steady stream of voice packets can be reproduced at the destination. The default jitter buffer delay for voice is 60 ms.

Other delay components

The following other delay components are generally considered very minor:

- router processing delay

  The time it takes to forward a packet from one link to another on the router is the transit or router processing delay. In a healthy network, router processing delay is approximately a few milliseconds.

- LAN segment delay

  The transmission and processing delay of packets through a healthy LAN subnet is approximately one or two milliseconds.

Reducing delays

Introduction

This section provides guidelines for reducing one-way delay and packet loss in the Remote Office network.

Reducing link delay

The time it takes for a voice packet to be queued on the transmission buffer of a link until it is received at the next hop router is the link delay. Link delay can be reduced by

- upgrading link capacity

  This reduces the serialization delay of the packet, but also more significantly, it reduces the utilization of the link and the queueing delay. To estimate how much delay can be reduced, refer to the tables and formulas given in "Serialization delay" on page 305 and "Queuing delay" on page 306.   Before upgrading a link, you must check both routers connected to the link intended for the upgrade and ensure that router configuration guidelines are complied with.
- changing the link from satellite to terrestrial

  This should reduce the link delay by 100 to 300 ms.
- implementing a priority queueing discipline

  See "Queue management" on page 314.

To determine which links should be considered for upgrading, first list all the intranet links used to support the Remote Office traffic, which can be derived from the traceroute output for each site pair. Then, using the intranet link utilization report, note the highest utilized or the slowest links, or both. Estimate the link delay of suspect links using the traceroute results.

Suppose that a 256 Kbps link from Router 1 to Router 2 has a high utilization. The following is a traceroute output that traverses this link:

```
Richardson3 % traceroute santa_clara_Remote Office4
traceroute to santa_clara_Remote Office4 (10.3.2.7), 30
```

```
hops max, 32 byte packets
Router 1 (10.8.0.1) 1 ms  1 ms  1 ms
Router 2 (10.18.0.2) 42 ms  44 ms  38 ms
Router 3 (10.28.0.3) 78 ms  70 ms  81 ms
Router 4 (10.3.0.1) 92 ms  90 ms  101 ms
santa_clara_Remote Office4 (10.3.2.7) 94 ms  97 ms  95
ms
```

The average *rtt* time on that link is about 40 ms. The one-way link delay is about 20 ms, of which the circuit transmission and serialization delay are just a few milliseconds. Most of this link’s delay is caused by queueing. Refer to “Queuing delay of various links” on page 306. If you upgrade this link to T1, you can shave about 19 ms off the delay budget.

Reducing hop count

You can significantly reduce end-to-end delay by reducing hop count, especially on hops that traverse WAN links. These are some of the ways to reduce hop count:

- Attach the TLAN directly to the WAN router.
- Improve meshing.

  Add links to help improve meshing. If you add a link from Router 1 to Router 4 in the previous traceroute example, this might cause the routing protocol to use that new link, thereby reducing the hop count by two.
- Reduce the number of nodes.

  You can connect collocated nodes into one larger and more powerful router.

These guidelines affect the whole intranet, as they tamper with network architecture, design, and policies. To proceed with this involves considering cost, and political and IP design issues—topics which are beyond the scope of this document.

Reducing packet errors

Packet errors in intranets are generally correlated with congestion somewhere in the network. Bottleneck links occur where the packet errors are high because packets get dropped when they arrive faster than the link can transmit them. The task of upgrading highly utilized links can remove the source of packet errors on a particular flow. Also, an effort to reduce hop count gives fewer opportunities for routers and links to drop packets.

Other causes of packet errors not related to queueing delay are as follows:

- poor link quality

  The underlying circuit can have transmission problems, high line error rates, be subject to frequent outages, and so on. Note that the circuit can be provisioned on top of other services, such as X.25, frame relay, or ATM. Check with the service provider for information.

- overloaded CPU

  This is another commonly monitored statistic collected by network management systems. If a router is overloaded, it means that the router is constantly performing processing-intensive tasks, which impedes the router from forwarding packets. Find out what the threshold CPU utilization level is, and check if any suspect router conforms to the threshold. The router might have to be reconfigured or upgraded.

- saturation

  Routers can be overworked when there are too many high-capacity and high-traffic links configured on it. Ensure that routers are dimensioned according to vendor guidelines.

- LAN saturation

  Packets can also be dropped on under-engineered or faulty LAN segments.

Routing issues

Routing irregularities can introduce unnecessary delay. A routing implementation can overlook a substantially better route. A high delay variation can be caused by routing instability, misconfigured routing, inappropriate load splitting, or frequent changes to the intranet. Severe asymmetrical routing results in one site perceiving a poorer QoS than the other.

You can use the traceroute program to uncover these routing anomalies. Subsequently, routing implementation and policies can be audited and corrected.

Network modeling

Network analysis can be difficult or time-consuming if the intranet and the expected Remote Office installation is large. To this end, commercial network modeling tools exist to analyze what-if scenarios of predicting the effect of topology, routing, and bandwidth changes to the network. They work with an existing network management system to load current configuration, traffic, and policies into the tool. Network modeling tools can help you analyze and try out any of the recommendations given in this document to predict how delay and error characteristics can change.

Implementing Quality of Service in IP networks

Introduction

Today's corporate intranets are developed because of the need to support data services, for which a "best effort" IP delivery mechanism usually suffices. Standard intranets are designed to support a set of QoS objectives dictated by these data services.

Setting Quality of Service objectives

When an intranet takes on a real-time service, the users of that service impose additional QoS objectives in the intranet. Some of these targets can be less stringent compared with those imposed by current services, while other targets are more stringent. For intranets not exposed to real-time services in the past but that now need to deliver Remote Office traffic, it is likely that the QoS objectives pertaining to delay will impose an additional design constraint on the intranet.

Method 1

One approach is to simply subject all intranet traffic to additional QoS constraints, and to design the network to the strictest QoS objectives. This is essentially a "best-of-breed" solution. This, for example, would improve the quality of data services, even though most applications might not perceive a reduction of 50 ms in delay. Improvements to the network result in one that would be adequately engineered for voice, but over-engineered for data services.

Method 2

Another approach is to consider using QoS mechanisms in the intranet, the goal of which is to provide a more cost-effective solution to engineering the intranet for non-homogenous traffic types. Unfortunately, IP QoS mechanisms are still relatively new, hardly implemented on intranets, and difficult to predict the consequences.

This section outlines what QoS mechanisms can work in conjunction with the Remote Office node, and with what new intranet-wide consequences if implemented.

Traffic mix

Before implementing QoS mechanisms in the network, you must assess the traffic mix of the network. QoS mechanisms depend on the process and ability to distinguish traffic (by class) so as to provide differentiated services.

If an intranet is designed solely to deliver Remote Office traffic, and all traffic flows are equal priority, then there is no need to consider QoS mechanisms. This network has only one class of traffic.

In most corporate environments, the intranet is primarily supporting data and other services. When planning to offer voice services over the intranet, you must assess the following:

- Are there existing QoS mechanisms? What kind? The Remote Office traffic should take advantage of established mechanisms, if possible.
- What is the traffic mix? If the Remote Office traffic is small compared to data traffic on the intranet, then IP QoS mechanisms can suffice. If Remote Office traffic is significant, then data services might be impacted when those mechanisms are biased toward Remote Office traffic.

TCP traffic behavior

The majority of corporate intranet traffic is TCP-based. Unlike UDP, which has no flow control, TCP uses a sliding window flow control mechanism. Under this scheme, TCP increases its window size, increasing throughput until congestion occurs. Congestion is detected by packet losses, and when that happens, the throughput is quickly throttled down, and the whole cycle repeats.

When multiple TCP sessions flow over few bottleneck links in the intranet, the flow control algorithm can cause TCP sessions in the network to throttle at the same time, resulting in a periodic and synchronized surge and ebb in traffic flows. WAN links appear to be congested at one time, and are then followed by a period of under-utilization. There are two consequences:

- poor efficiency of WAN links
- unfairly affected Remote Office traffic streams

Queue management

From “Queuing delay” on page 306, you can see that queueing delay is a major contributor to delay, especially on highly utilized and low-bandwidth WAN links. Routers that are TOS-aware and support class-based queuing can help reduce queueing delay of voice packets when these packets are treated with preference over other packets. To this end, Class-Based Queueing (CBQ) can be considered for implementation on these routers, with the Remote Office traffic prioritized against other traffic.

Class-based queueing, however, can be CPU-intensive and might not scale well when applied on high-bandwidth links. Thus, if this is to be implemented for the first time on the intranet, do so selectively. Usually, CBQ is implemented at edge or entry routers.

The global synchronization situation described in “TCP traffic behavior” on page 313 can be countered using a buffer management scheme, which discards packets randomly as the queue starts to exceed some threshold. Weighted Random Early Detection (WRED), an implementation of this strategy, additionally inspects the TOS bits in the IP header when considering which packets to drop during buffer buildup. In an intranet environment where TCP traffic dominates real-time traffic, WRED can be used to maximize the dropping of packets from long-lived TCP sessions and minimize the dropping of voice packets.

As in CBQ, check the configuration guidelines with the router vendor for performance ramifications when enabling WRED. If global synchronization is to be countered effectively, WRED should be implemented at core and edge routers.

Use of Frame Relay and ATM services

IP can be transported over Frame Relay and ATM services, both of which provide QoS-based delivery mechanisms. If the router can discern Remote Office traffic by inspecting the TOS field or observing the UDP port numbers, it can forward the traffic to the appropriate Permanent Virtual Circuit (PVC) or Switched Virtual Circuit (SVC). At the data link layer, the differentiated virtual circuits need to be provisioned. In Frame Relay, the differentiation is created by having both zero-Committed Information Rate (CIR) and CIR-based PVCs. In ATM, differentiation is created by having virtual circuits with different QoS classes.

Internet Protocols and ports used by Remote Office

The following IP applications and protocols are used by Remote Office and must be transmitted across your intranet by all IP routers and other network equipment:

- TCP port 12800
- UDP ports
- proprietary trunk protocol and High Level Data Link Control (HDLC) encapsulation
- IP stack

This information should be validated and included in the Remote Office network engineering guidelines.

TCP port 12800

Remote Office uses well-known TCP port 12800 to establish a signaling session over TCP between the MIG RLC and each Remote Office 9150 unit. The encapsulation over TCP is a proprietary format that encodes the X.11 signaling.

UDP ports

Remote Office uses two well-known UDP ports to establish TCP sessions. It uses 20482 for testing during QoS transition recovery. It uses 20480 to multiplex all the active voice traffic. The formats of the voice and pseudo-port traffic are both proprietary. They contain a 12-byte header in addition to the voice payload, which is dependent upon the algorithm (for example, G729). Each voice packet contains 30 milliseconds of voice payload, so the size of the voice packet varies according to the algorithm used.

Proprietary trunk protocol and HDLC encapsulation

Remote Office uses a proprietary trunk protocol when communicating over ISDN, and HDLC encapsulation when transferring packetized voice. Both the signaling and voice payloads are multiplexed over the same channel. Further, the multi-link protocol allows distribution of the information over several independent B-channels. The protocol uses a compressed voice header so that, in best-case scenarios, only five bytes of overhead (opening and closing HDLC flag, 16-bit CRC, and 1-byte header) are used in addition to the payload.

IP stack

The IP stack does not contain a routing protocol. It relies on the default gateway to do routing. It is fully compliant to IP Version 4 and supports ICMP and ARP. It is compatible with Ethernet 802.3 and Ethernet II networks.

Appendix B

Planning forms

In this appendix

Overview

Introduction

This appendix provides several forms on which you can plan and record the various data necessary for proper configuration of each MIG RLC at your site. For your reference, forms are also provided for the Remote Office 9150 unit.

Network planning

To help you plan your Remote Office network, study the information provided in Appendix C, “Sample configuration files,”on page 357. Study the network diagram and the sample configuration files. The information provided in the appendix demonstrates the relationships between the MIG RLC and the Remote Office 9150 configuration settings.

Remote Office 9150 forms

Use the Remote Office 9150 forms to record information and calculate needed resources for a Remote Office 9150 unit. For more information about using these forms, see the “Planning for installation” chapter in the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215).

MIG RLC forms

Use the Meridian Internet Gateway Reach Line Card forms to record information and calculate needed resources for the MIG RLC. They are provided in this guide for reference only.

For more information about using these forms, refer to the *Meridian Internet Gateway Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

Data entry form completion sequence

Information from some forms might need to be copied to other forms. Generally, you should complete the data entry forms in the following sequence:

1. Remote Office 9150 Configuration Information—Stations form
2. Meridian Internet Gateway Reach Line Card Connection Information (for either the 16-port or 32-port MIG RLC)
3. Remote Office 9150 Configuration Information—Network Connections form
4. Remote Office 9150 Configuration Information—ISDN BRI Modules form
5. Remote Office 9150 Configuration Information—Dialing Plans form
6. Meridian Internet Gateway Reach Line Card Online/Offline Table Configuration (if required)

   For more details, see

   - “Completing the Remote Office 9150 forms” on page 342
   - “Completing the MIG RLC forms” on page 322

Section A: Meridian Internet Gateway Reach Line Card forms

In this section

Completing the MIG RLC forms

Introduction

This section briefly describes how to complete the MIG RLC configuration forms.

To complete the forms

ATTENTION

Before you can assign MIG RLC ports to remote users, you must determine the remote user requirements. Do this by starting with the Remote Office 9150 Configuration Information—Stations form. See step 1 on page 342.

1 Assign users on the Remote Office 9150 unit to remote ports on the MIG RLC.

Note: To do this effectively, complete the Remote Office 9150 Configuration Information—Stations form first. See step 1 on page 342.

Record the MIG RLC port assignments in the “Port configuration” section on one of the following MIG RLC forms (according to the type of MIG RLC installed):

- Connection Information—16 ports
- Connection Information—32 ports

Users who are using an MCA to transmit data must be assigned to a PBX data port. Users who are using ATAs can be assigned to PBX voice or data ports. Configure ATA users as voice ports only if there are not enough free data ports. See “Remote port configuration” on page 106 for more information.

Note: The Connection Information forms identify the maximum number of ports that can be associated with MCAs and ATAs that are used to transmit data.

2 If you want to route calls over the circuit-switched network, designate MIG RLC ports to be used as network ports. At the same time, identify the telephone number that will be used to establish the connection with the Remote Office 9150 unit.

Note: Network ports must be assigned to PBX data ports.

Record the network port assignments and remote unit PSTN numbers on the Connection Information form for your MIG RLC type.

3 Record the IP address for each Remote Office 9150 unit on the Connection Information form for your MIG RLC type.

4 If the chosen security level is *security code*, record the security identifier that each remote unit will use to validate connection requests.

Note: The chosen security level must be the same on both the MIG RLC and remote unit.

5 On the same form, record the following items for the MIG RLC in the "Reach Line Card information" section:

- IP address, subnet mask, and gateway
- security level, and if required, security identifier

6 If necessary, complete a MIG RLC Online/Offline Table Configuration form for each remote unit.

Note: This step is optional.

Meridian Internet Gateway Reach Line Card

Connection Information—16 ports

Complete one copy of this form for each Line Card.

Page 1 of 5

Reach Line Card information

IPE position: Loop:________ Shelf: _______________ Card:____________

IP address: □□□.□□□.□□□.□□□

Subnet mask: □□□.□□□.□□□.□□□

Default gateway: □□□.□□□.□□□.□□□

Meridian 1 PBX's ELAN IP address: □□□.□□□.□□□.□□□

Meridian 1 PBX's ELAN subnet mask: □□□.□□□.□□□.□□□

Security level: ❐ No security is required ❐ Caller ID ❐ Security Code

If the security level is *security code,* MIG RLC's security identifier: ____________________

Port configuration

Notes:

- This Reach Line Card provides 32 digital telephone ports that can be configured as voice or data. Ports configured as Network connection or Remote user using MCA (for data transmission) or FAX must be configured on the host PBX with data capability. Ports configured as Remote user using ATA can be assigned to voice ports if there are not enough free data ports.
- If MCAs or ATAs will be used to transmit data, a maximum of four MCAs or ATAs can be connected to this Reach Line Card.

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address (if Network port)	Security ID (if Network port)
0	❐ Network connection ❐ Remote user ❐ Local telephone	❐ Yes ❐ No			
1	❐ Network connection ❐ Remote user ❐ Local telephone	❐ Yes ❐ No			

Meridian Internet Gateway Reach Line Card

Connection Information—16 ports

Port configuration (continued)

Page 2 of 5

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address (if Network port)	Security ID (if Network port)
2	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
3	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
4	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
5	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
6	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
7	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
8	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
9	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
10	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			

Meridian Internet Gateway Reach Line Card

Connection Information—16 ports

Port configuration (continued)

Page 3 of 5

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address (if Network port)	Security ID (if Network port)
11	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
12	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
13	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
14	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
15	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
16	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
17	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
18	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
19	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			

Meridian Internet Gateway Reach Line Card

Connection Information—16 ports

Port configuration (continued) **Page 4 of 5**

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address (if Network port)	Security ID (if Network port)
20	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
21	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
22	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
23	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
24	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
25	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
26	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
27	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
28	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			

Meridian Internet Gateway Reach Line Card

Connection Information—16 ports

Port configuration (continued) **Page 5 of 5**

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address (if Network port)	Security ID (if Network port)
29	❐ Network connection ❐ Remote user ❐ Local telephone	❐ Yes ❐ No			
30	❐ Network connection ❐ Remote user ❐ Local telephone	❐ Yes ❐ No			
31	❐ Network connection ❐ Remote user ❐ Local telephone	❐ Yes ❐ No			

Meridian Internet Gateway Reach Line Card

Connection Information—32 ports

Complete one copy of this form for each Line Card. **Page 1 of 8**

Reach Line Card information

IPE position: Loop:________ Shelf: _______________ Card:____________

IP address: □□□.□□□.□□□.□□□

Subnet mask: □□□.□□□.□□□.□□□

Default gateway: □□□.□□□.□□□.□□□

Meridian 1 PBX’s ELAN IP address: □□□.□□□.□□□.□□□

Meridian 1 PBX’s ELAN subnet mask: □□□.□□□.□□□.□□□

Security level: □ No security is required □ Caller ID □ Security Code

If the security level is *security code*, MIG RLC’s security identifier: ______________________

Port configuration

Notes:

- This Reach Line Card provides 64 digital telephone ports that can be configured as voice or data. Ports configured as Network connection or Remote user using MCA (for data transmission) or FAX must be configured on the host PBX with data capability. Ports configured as Remote user using ATA can be assigned to voice ports if there are not enough free data ports.
- If MCAs or ATAs will be used to transmit data, a maximum of seven MCAs or ATAs can be connected to this Reach Line Card.

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address (if Network port)	Security ID (if Network port)
Slot 1					
0	□ Network connection □ Remote user □ Local telephone	□ Yes □ No			

Meridian Internet Gateway Reach Line Card

Connection Information—32 ports

Port configuration (continued) **Page 2 of 8**

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address (if Network port)	Security ID (if Network port)
1	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
2	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
3	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
4	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
5	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
6	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
7	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
8	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
9	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			

Meridian Internet Gateway Reach Line Card

Connection Information—32 ports

Port configuration (continued) **Page 3 of 8**

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address (if Network port)	Security ID (if Network port)
10	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
11	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
12	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
13	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
14	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
15	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
16	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
17	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
18	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			

Meridian Internet Gateway Reach Line Card

Connection Information—32 ports

Port configuration (continued) **Page 4 of 8**

RLC port number	**Port type**	**MCA, ATA, or FAX?**	**PSTN number (if Network port)**	**IP address (if Network port)**	**Security ID (if Network port)**
19	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
20	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
21	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
22	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
23	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
24	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
25	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
26	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
27	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			

Meridian Internet Gateway Reach Line Card

Connection Information—32 ports

Port configuration (continued) **Page 5 of 8**

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address (if Network port)	Security ID (if Network port)
28	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
29	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
30	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
31	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
Slot 2					
32	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
33	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
34	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
35	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
36	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			

Meridian Internet Gateway Reach Line Card

Connection Information—32 ports

Port configuration (continued) **Page 6 of 8**

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address (if Network port)	Security ID (if Network port)
37	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
38	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
39	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
40	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
41	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
42	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
43	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
44	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
45	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			

Meridian Internet Gateway Reach Line Card

Connection Information—32 ports

Port configuration (continued) **Page 7 of 8**

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address (if Network port)	Security ID (if Network port)
46	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
47	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
48	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
49	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
50	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
51	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
52	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
53	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
54	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			

Meridian Internet Gateway Reach Line Card

Connection Information—32 ports

Port configuration (continued) **Page 8 of 8**

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address (if Network port)	Security ID (if Network port)
55	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
56	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
57	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
58	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
59	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
60	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
61	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
62	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			
63	❒ Network connection ❒ Remote user ❒ Local telephone	❒ Yes ❒ No			

Meridian Internet Gateway Reach Line Card

Online/Offline Table Configuration

Page 1 of 1

MIG RLC port number: ________________ Remote unit number: ________________

Notes:

- If a schedule is not defined for this remote site, the digital telephone online/offline status is defined solely by the remote site user dialing the online/offline SPRE code on the telephone.
- The schedule, if configured, does not prevent this site from establishing or terminating a connection to the network. Schedule entries can be overridden by the site user by dialing the online/offline SPRE code on the telephone.

Day	On	Off	On	Off	On	Off	On	Off
Monday	_______	_______	_______	_______	_______	_______	_______	_______
	_______	_______	_______	_______	_______	_______	_______	_______
Tuesday	_______	_______	_______	_______	_______	_______	_______	_______
	_______	_______	_______	_______	_______	_______	_______	_______
Wednesday	_______	_______	_______	_______	_______	_______	_______	_______
	_______	_______	_______	_______	_______	_______	_______	_______
Thursday	_______	_______	_______	_______	_______	_______	_______	_______
	_______	_______	_______	_______	_______	_______	_______	_______
Friday	_______	_______	_______	_______	_______	_______	_______	_______
	_______	_______	_______	_______	_______	_______	_______	_______
Saturday	_______	_______	_______	_______	_______	_______	_______	_______
	_______	_______	_______	_______	_______	_______	_______	_______
Sunday	_______	_______	_______	_______	_______	_______	_______	_______
	_______	_______	_______	_______	_______	_______	_______	_______

Meridian Internet Gateway Reach Line Card

System expansion worksheet

Page 1 of 2

Complete one worksheet for each MIG RLC.

1 How many remote users will be supported?
Notes:

- Up to 16 users can be connected to the NTDR68AA Line Card. Up to 32 users can be connected to the NTDR70AA or NTDR71AA Line Cards.
- If ATAs or MCAs will be used to transmit data, up to four ATAs or MCAs can be supported on the NTDR68AA Line Card. Up to seven ATAs or MCAs can be supported on the NTDR70AA or NTDR71AA Line Cards. Each ATA requires the resources of one DSP channel for data transmission.

____

2 Do you want to implement call blocking? (Users will receive a fast busy signal when resources are not available.) ❒ Yes ❒ No

3 If line 7 is Yes, calculate the number of calls that can be active at one time.
Note: A conservative estimate of one call in three being blocked when no resources are available is recommended.)
Multiply line 1 by your call blocking factor. For example, to calculate the number of simultaneous calls that can be supported at a 3 to 2 blocking ratio, multiply line 1 by 2/3 (0.666). If the result contains a fraction, round up to a whole number.

Line 1: _________ x ___________ = _______________

If line 7 is No, the number of simultaneous calls is the same as the number of user stations installed. (Record your response to line 1 here.) ___________

Number of DSP application modules needed

Notes:

- If the MIG RLC supports only one Remote Office 9150 unit, the number of DSP application modules installed on the MIG RLC must be the same as the number of modules installed on the Remote Office 9150 unit.
- If the MIG RLC is supporting more than one site, the number of DSP applications modules you need must support the voice processing capability for all sites combined.

4 Divide line 8 by 8, then round up the result to a whole number.
Line 8: _____________ / 8 = _______________ ___________

Meridian Internet Gateway Reach Line Card

System expansion worksheet

Page 2 of 2

Number of DSP application modules needed (continued)

5 Record the number of DSP application modules already installed.
Note: The MIG RLC shipped from Nortel Networks with one DSP module already installed. Your response here must *include* that module. ____________

6 Calculate how many DSP modules you need to purchase.
Subtract line 18 from line 17.
Note: Only one DSP application module can be installed on the NTDR68AA Line Card. Up to three DSP application modules can be installed on the NTDR70AA or NTDR71AA Line Cards. ____________

7 Allow for future growth? ❐ Yes ❐ No

Note: All Remote Office 9150 unit users must be assigned to one MIG RLC only. Therefore, future assignment of MIG RLC ports should be considered.

For example, if the number of users for a Remote Office 9150 unit grows from 8 to 20, and 12 more ports are not available on the MIG RLC, then a complete reassignment of the Remote Office 9150 unit (20 users) to another MIG RLC is required.

Section B: Remote Office 9150 forms

In this section

Completing the Remote Office 9150 forms

Introduction

This section briefly describes how to complete the Remote Office 9150 configuration forms.

To complete the forms

1 Assign each user telephone or fax machine to a port on the Remote Office 9150 unit.

Record the assignments on the Remote Office 9150 Configuration Information—Stations form. Designate each port as a local port, remote port, or local and remote port.

2 Use the information you received from the ISDN service provider for the Remote Office 9150 site to complete the Remote Office 9150 Configuration Information—ISDN BRI Modules form.

At the same time, do the following:

a. Designate a B-channel as a primary trunk. The Remote Office 9150 unit uses primary trunk to establish connections between the Remote Office 9150 unit and the MIG RLC.

Note: B-channel 1 on module 4 is designated by default as the primary trunk.

b. Record the primary trunk assignment in the “Connection to MIG RLC information” section on the Remote Office 9150 Configuration Information—Network Connections form.

c. Assign B-channels to trunk groups. Record the assignments on the ISDN BRI Modules form.

3 Assign an IP address, subnet mask, and gateway to the Remote Office 9150 unit. This information is required if you want to administer the Remote Office 9150 unit over the IP network.

Record the addresses in the “Remote Office 9150 unit identification” section on the Remote Office 9150 Configuration Information—Network Connections form.

4 If the security level chosen is *security code*, record the security identifier assigned to the Remote Office 9150 unit.

5 In the “Connection to MIG RLC information” section on the Remote Office 9150 Configuration Information—Network Connections form, record the MIG RLC’s

- IP address
- telephone number
- security code

The Remote Office 9150 unit uses this information to establish and authenticate connections with the MIG RLC.

6 If an online/offline table is configured on the MIG RLC, configure the SPRE codes for toggling the online/offline modes on the Remote Office 9150 unit.

Note: This step is optional, because default SPRE codes have already been defined in the software (as indicated on the Remote Office 9150 Configuration Information—Dialing Plans form).

If you choose to change the code, record the new code on the Dialing Plans form.

7 Define the trunk access and Paging SPRE codes.

Trunk access codes are used by Remote Office 9150 unit users to get outside lines.

Note: Default trunk access digits and paging SPRE codes have already been defined. Nortel Networks recommends that you use the defaults.

If you choose to change the predefined codes, record them on the Remote Office 9150 Configuration Information—Dialing Plans form. Also, record the trunk access codes (as required) on the ISDN BRI Modules form.

Remote Office 9150

Configuration Information—Stations

Page 1 of 4

Notes:

- A maximum of seven MCAs and ATAs can be connected to digital telephones at this site.
- If you are connecting a fax machine or analog device that is not equipped with an ATA, it can be connected only to port 64. If you want to connect a fax machine or analog device to any other port, it must be equipped with an ATA.

9150 port #	Extension number (DN)		Type		If a remote port, host port number (TN)	MCA or ATA?	
0		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
1		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
2		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
3		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
4		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
5		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
6		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
7		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
8		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
9		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
10		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
11		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
12		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
13		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
14		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
15		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
16		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
17		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
18		❒ Local	❒Remote	❒Both		❒ Yes	❒ No

Remote Office 9150

Configuration Information—Stations

Page 2 of 4

Notes:

- A maximum of seven MCAs and ATAs can be connected to digital telephones at this site.
- If you are connecting a fax machine or analog device that is not equipped with an ATA, it can be connected only to port 64. If you want to connect a fax machine or analog device to any other port, it must be equipped with an ATA.

9150 port #	**Extension number (DN)**	**Type**			**If a remote port, host port number (TN)**	**MCA or ATA?**	
19		□ Local	□Remote	□Both		□ Yes	□ No
20		□ Local	□Remote	□Both		□ Yes	□ No
21		□ Local	□Remote	□Both		□ Yes	□ No
22		□ Local	□Remote	□Both		□ Yes	□ No
23		□ Local	□Remote	□Both		□ Yes	□ No
24		□ Local	□Remote	□Both		□ Yes	□ No
25		□ Local	□Remote	□Both		□ Yes	□ No
26		□ Local	□Remote	□Both		□ Yes	□ No
27		□ Local	□Remote	□Both		□ Yes	□ No
28		□ Local	□Remote	□Both		□ Yes	□ No
29		□ Local	□Remote	□Both		□ Yes	□ No
30		□ Local	□Remote	□Both		□ Yes	□ No
31		□ Local	□Remote	□Both		□ Yes	□ No

Use ports 32 through 63 only if this Remote Office 9150 unit connects to a 2-slot MIG RLC on the host PBX.

32		□ Local	□Remote	□Both		□ Yes	□ No
33		□ Local	□Remote	□Both		□ Yes	□ No
34		□ Local	□Remote	□Both		□ Yes	□ No
35		□ Local	□Remote	□Both		□ Yes	□ No

Remote Office 9150

Configuration Information—Stations

Page 3 of 4

Notes:

- A maximum of seven MCAs and ATAs can be connected to digital telephones at this site.
- If you are connecting a fax machine or analog device that is not equipped with an ATA, it can be connected only to port 64. If you want to connect a fax machine or analog device to any other port, it must be equipped with an ATA.

9150 port #	Extension number (DN)	Type			If a remote port, host port number (TN)	MCA or ATA?	
36		❐ Local	❐Remote	❐Both		❐ Yes	❐ No
37		❐ Local	❐Remote	❐Both		❐ Yes	❐ No
38		❐ Local	❐Remote	❐Both		❐ Yes	❐ No
39		❐ Local	❐Remote	❐Both		❐ Yes	❐ No
40		❐ Local	❐Remote	❐Both		❐ Yes	❐ No
41		❐ Local	❐Remote	❐Both		❐ Yes	❐ No
42		❐ Local	❐Remote	❐Both		❐ Yes	❐ No
43		❐ Local	❐Remote	❐Both		❐ Yes	❐ No
44		❐ Local	❐Remote	❐Both		❐ Yes	❐ No
45		❐ Local	❐Remote	❐Both		❐ Yes	❐ No
46		❐ Local	❐Remote	❐Both		❐ Yes	❐ No
47		❐ Local	❐Remote	❐Both		❐ Yes	❐ No
48		❐ Local	❐Remote	❐Both		❐ Yes	❐ No
49		❐ Local	❐Remote	❐Both		❐ Yes	❐ No
50		❐ Local	❐Remote	❐Both		❐ Yes	❐ No
51		❐ Local	❐Remote	❐Both		❐ Yes	❐ No
52		❐ Local	❐Remote	❐Both		❐ Yes	❐ No
53		❐ Local	❐Remote	❐Both		❐ Yes	❐ No

Remote Office 9150

Configuration Information—Stations

Page 4 of 4

Notes:

- A maximum of seven MCAs and ATAs can be connected to digital telephones at this site.
- If you are connecting a fax machine or analog device that is not equipped with an ATA, it can be connected only to port 64. If you want to connect a fax machine or analog device to any other port, it must be equipped with an ATA.

9150 port #	Extension number (DN)	Type			If a remote port, host port number (TN)	MCA or ATA?	
54		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
55		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
56		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
57		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
58		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
59		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
60		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
61		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
62		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
63		❒ Local	❒Remote	❒Both		❒ Yes	❒ No
64: FAX		❒ Local	❒Remote	❒Both		❒ Yes	❒ No

Remote Office 9150

Configuration Information—ISDN BRI Modules

Page 1 of 3

Module 4

ISDN line type (variant): Switch type:

B-channel 1 DN: SPID:

Allocation:
❒ Permanent ❒ Demand

Connection type:
❒ Local ❒ Local and Remote
❒ Remote

Trunk group: Trunk access code:

B-channel 2 DN: SPID:

Allocation:
❒ Permanent ❒ Demand

Connection type:
❒ Local ❒ Local and Remote
❒ Remote

Trunk group: Trunk access code:

Module 5

ISDN line type (variant): Switch type:

B-channel 1 DN: SPID:

Allocation:
❒ Permanent ❒ Demand

Connection type:
❒ Local ❒ Local and Remote
❒ Remote

Trunk group: Trunk access code:

Remote Office 9150

Configuration Information—ISDN BRI Modules

Page 2 of 3

Module 5 (continued)

B-channel 2 DN: ____________________________ SPID: ______________________________

Allocation: □ Permanent □ Demand

Connection type: □ Local □ Local and Remote □ Remote

Trunk group: ____________________________ Trunk access code: ______________________________

Module 6

ISDN line type (variant): ____ Switch type: ______________________________

B-channel 1 DN: ____________________________ SPID: ______________________________

Allocation: □ Permanent □ Demand

Connection type: □ Local □ Local and Remote □ Remote

Trunk group: ____________________________ Trunk access code: ______________________________

B-channel 2 DN: ____________________________ SPID: ______________________________

Allocation: □ Permanent □ Demand

Connection type: □ Local □ Local and Remote □ Remote

Trunk group: ____________________________ Trunk access code: ______________________________

Remote Office 9150

Configuration Information—ISDN BRI Modules

Page 3 of 3

Module 7

ISDN line type (variant): ______________________________ Switch type: ______________________________

B-channel 1 DN: ______________________________ SPID: ______________________________

Allocation:
❒ Permanent ❒ Demand

Connection type:
❒ Local ❒ Local and Remote
❒ Remote

Trunk group: ______________________________ Trunk access code: ______________________________

B-channel 2 DN: ______________________________ SPID: ______________________________

Allocation:
❒ Permanent ❒ Demand

Connection type:
❒ Local ❒ Local and Remote
❒ Remote

Trunk group: ______________________________ Trunk access code: ______________________________

Remote Office 9150

Configuration Information—Network Connections

Page 1 of 1

Security level: ❒ No security ❒ Caller ID ❒ Security code

Remote Office 9150 unit identification

Node number: ______________________ Node name: __________________________

IP address: ____.____.____.____

Subnet mask: ____.____.____.____

Default gateway: ____.____.____.____

If the security level is *security code*, what is the Remote Office 9150 unit's security identifier?

____

Connection to MIG RLC information

IP address to reach the host PBX (for IP network):

____.____.____.____

Telephone number to reach host PBX
(for circuit-switched network): __________________________

If security level is *security code*, what is the
MIG RLC's security identifier? __________________________

Trunk dedicated as the primary trunk:
Note: Refer to the Remote Office 9150 Configuration Information—ISDN BRI Modules form.

Module: ❒ 4 ❒ 5 ❒ 6 ❒ 7

B-channel ❒ 1 ❒ 2

Remote Office 9150

Configuration Information—Dialing Plans

Page 1 of 1

Notes:

- Nortel Networks recommends that you use the preconfigured default codes listed below.
- The pound sign (# in North America) is mandatory and is automatically preconfigured in Configuration Manager. The pound sign prevents conflicts with the dialing plan on the host PBX.
- You can dedicate all B-channels to one trunk group. You do not have to create a trunk group for each B-channel.

Description	Default code	Your code (maximum of 3 digits)
Online SPRE code	#99	#
Offline SPRE code	#98	#
Paging SPRE code	#05	#
Local Calling SPRE code (for analog or ATA-equipped stations)	#8	#
Registration SPRE code (for multi-user or dynamic pool ports only)	#97	#
Deregistration SPRE code (for multi-user or dynamic pool ports only)	#96	#
Access code for trunk group 1	#61	#
Access code for trunk group 2	#62	#
Access code for trunk group 3	#63	#
Access code for trunk group 4	#64	#
Access code for trunk group 5	#65	#
Access code for trunk group 6	#66	#
Access code for trunk group 7	#67	#
Access code for trunk group 8	#68	#

Remote Office 9150

System expansion worksheet

Page 1 of 3

Complete one worksheet for each Remote Office 9150 unit.

Number of stations:

1 How many digital telephones will be installed at the Remote Office 9150 site? **Note:** A maximum of 32 digital telephones can be connected to the Remote Office 9150 unit. ___________

2 How many Analog Telephone Adapters (ATAs) will be installed? ___________

3 How many Meridian Communication Adapters (MCAs) will be installed? ___________

4 Add lines 1 and 2 together. ___________

Notes:

- ■ A maximum of four MCAs and ATAs can be installed when connecting the Remote Office 9150 unit to a 1-slot MIG RLC. A maximum of seven MCAs and ATAs can be installed when connecting to a 2-slot MIG RLC.
- ■ The total number of ATAs and digital telephones cannot exceed 32. ___________

5 Will a fax machine be used for faxes through the host PBX? ❐ Yes ❐ No

6 If line 5 is Yes, add 1 to line 4. ___________

Call blocking:

7 Do you want to implement call blocking? (Users will receive a fast busy signal when resources are not available.) ❐ Yes ❐ No

8 If line 7 is Yes, calculate the number of calls that can be active at one time. **Note:** A conservative estimate of one call in three being blocked when no resources are available is recommended. Multiply line 4 by your call blocking factor. For example, to calculate the number of simultaneous calls that can be supported at a 3:2 blocking ratio, multiply line 6 by 2/3 (0.666). If the result contains a fraction, round up to a whole number.

Line 6: _________ x ___________ = _______________

If line 7 is No, the number of simultaneous calls is the same as the number of stations installed. (Record your response to line 6 here.) ___________

Remote Office 9150

System expansion worksheet

Page 2 of 3

Call routing:

9 How do you want to route host-controlled calls?

❒ IP network ❒ Circuit-switched network ❒ Both

Note: If you want to route host-controlled calls over both networks, then the QoS transitioning technology can be used.

10 If line 9 is Circuit-switched network or Both, do you want to support local-controlled calls through the circuit-switched network (that is, support local calling)? ❒ Yes ❒ No

Number of trunk interface modules needed for QoS transition support or routing calls over the circuit-switched network:
Note: If you are routing calls over the IP network only, skip this section.

11 If line 10 is No, enter 0.

If line 10 is Yes, how many simultaneous digital telephone or ATA local calls do you want to support?
Enter a value between 1–7.
Note: Only one active call per ISDN BRI B-channel is allowed in local-controlled mode because local calls are not compressed. ____________

12 Calculate the number of B-channels required for simultaneous calls in host-controlled mode.

Each B-channel can support one MCA call, or up to eight simultaneous voice calls using G.729A compression (where each call is compressed to 8 Kbps). However, when using G.729A compression, the first B-channel can support only six simultaneous calls because 16 Kbps are required for transporting call signaling data for the entire Remote Office 9150 unit (and all of its connected stations) to the host PBX.

Line 3: ________ + ((# of simultaneous calls: _______ * 8 Kbps) +
16 Kbps) / 64 = __________

Round up the result to a whole number. ____________

Remote Office 9150

System expansion worksheet

Page 3 of 3

Number of trunk interface modules needed (continued):

13 Calculate the number of B-channels required for both local- and host-controlled calls. Add lines 11 and 12.

If the result is greater than 8, then call blocking must be implemented, or the number of simultaneous local calls must be reduced.

Recalculate lines 8, 11, 12, and 13. ___________

14 Calculate the number of trunk interface modules required for local calls. Divide line 13 by 2. If the result contains a fraction, round it up to the next whole number.

Line 13: __________ / 2 = ____________ ___________

15 How many trunk interface modules are already installed in the Remote Office 9150 unit? ___________

16 Calculate the number of trunk interface modules you need to purchase. Subtract line 15 from line 14. ___________

Note: A maximum of four trunk interface modules can be installed in the Remote Office 9150 unit.

Number of DSP application modules needed:

17 Each DSP application module can support up to eight simultaneous calls over the IP network.

Divide line 8 by 8, and then round up the result to a whole number.
Line 8: _____________ / 8 = ______________ ___________

18 Record the number of DSP application modules already installed.
Note: The Remote Office 9150 unit ships from Nortel Networks with one DSP module already installed. Your response here must *include* that module. ___________

19 Calculate how many DSP modules you need to purchase.
Subtract line 18 from line 17.
Note: A maximum of three DSP application modules can be installed in the Remote Office 9150 unit. ___________

Appendix C

Sample configuration files

In this appendix

Example of a network

Introduction

This section provides an example of a network diagram that shows one host site (MIG RLC installed on the host PBX) and one Remote Office 9150 unit (with one user station). The purpose of this diagram is to demonstrate the relationship between configuration settings on each unit in the network.

Sample configuration printouts

Sample Meridian 1 PBX configuration printouts for the voice and data ports are provided as follows:

- voice port: on page 360
- data port: on page 362

Sample configuration printouts for the MIG RLC and Remote Office 9150 unit are shown as follows:

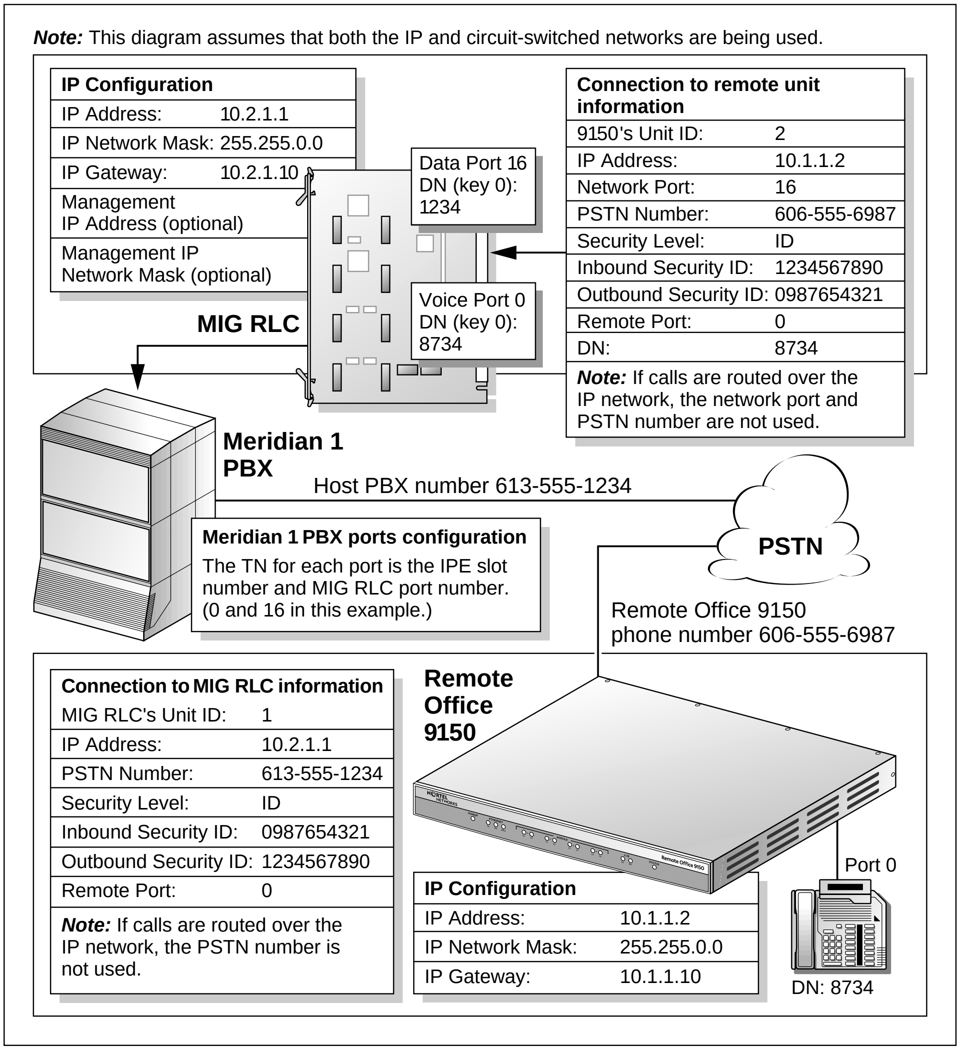
- MIG RLC: on page 364
- Remote Office 9150 unit: on page 368

Configuration recommendation

The quickest way to configure the MIG RLC and Remote Office 9150 unit is to run the Configuration Wizard. For instructions, see “Using the Configuration Wizard to perform initial configuration” on page 67. For your reference, the Configuration Wizard screen examples are completed using the same information.

Note: The network diagram shows information that cannot be configured through the Configuration Wizard, such as the security identifiers. You must use Configuration Manager to complete the configuration.

Network diagram



Note: This diagram assumes that both the IP and circuit-switched networks are being used.

IP Configuration	
IP Address:	10.2.1.1
IP Network Mask:	255.255.0.0
IP Gateway:	10.2.1.10
Management IP Address (optional)	
Management IP Network Mask (optional)	

Connection to remote unit information	
9150's Unit ID:	2
IP Address:	10.1.1.2
Network Port:	16
PSTN Number:	606-555-6987
Security Level:	ID
Inbound Security ID:	1234567890
Outbound Security ID:	0987654321
Remote Port:	0
DN:	8734

Note: If calls are routed over the IP network, the network port and PSTN number are not used.

Data Port 16
DN (key 0):
1234

Voice Port 0
DN (key 0):
8734

Meridian 1 PBX ports configuration

The TN for each port is the IPE slot number and MIG RLC port number. (0 and 16 in this example.)

Connection to MIG RLC information	
MIG RLC's Unit ID:	1
IP Address:	10.2.1.1
PSTN Number:	613-555-1234
Security Level:	ID
Inbound Security ID:	0987654321
Outbound Security ID:	1234567890
Remote Port:	0

Note: If calls are routed over the IP network, the PSTN number is not used.

IP Configuration	
IP Address:	10.1.1.2
IP Network Mask:	255.255.0.0
IP Gateway:	10.1.1.10

G101413

Voice port configuration on the Meridian 1 PBX

Introduction

This section shows the configuration settings for the voice port on the Meridian 1 PBX. Generally, define voice ports according to the needs of your remote users.

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 359.

Note: This configuration example is from a Meridian 1 Option 11.

```
REQ: prt
TYPE: 2616                            Telephone type
MARP NOT ACTIVATED

TN   5 0
DATE
PAGE
DES

DES  Bryan Dion
TN   005 0 00 00                      MIG RLC slot and port numbers
TYPE 2616
CDEN 8D
CUST 0
AOM  0
FDN
TGAR 1
LDN  NO
NCOS 0
SGRP 0
RNPG 0
SCI  0
SSU
XLST
```

```
CLS  CTD FBD WTA LPR MTD FND HTD ADD HFD
     MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD DSX VMD CMSD CCSD SWD LND CNDD
     CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
     ICDD CDMD LLCN MCTD CLBD AUTU
     GPUD DPUD DNDD CFXD ARHD CLTD ASCD
      CPFA CPTA ABDD CFHD FICD NAID BUZZ AHD
      DDGA NAMA
      DRDD EXR0
      USMD USRD ULAD RTDD RBDD RBHD PGND FLXD FTTC DNDY DNO3
CPND_LANG ENG
HUNT
PLEV 02
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
DNDR 0
KEY  00 SCR 8734 0     MARP
        CPND
          NAME Bryan Dion
          XPLN 24
          DISPLAY_FMT FIRST,LAST
     01 CWT
     02 MSB
     03 TRN
     04 CFW 4
     05 AO6
     06
     07
     08
     09
     10 MCR 8234 0 MARP
        CPND
          NAME Bryan Dion
          XPLN 24
          DISPLAY_FMT FIRST,LAST
     11 AO6
     12
     13 DSP
     14
     15
```

VCE defines the port as a voice port.

9150 unit user’s DN

9150 unit user’s CPND

Data port configuration on the Meridian 1 PBX

Introduction

This section shows the configuration settings for the data port on the Meridian 1 PBX. The data port provides the communication path between the MIG RLC and the Remote Office 9150 unit, and must be configured as an MCA adapter.

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 359.

Note: This configuration sample is from a Meridian 1 Option 11.

```
REQ: prt
TYPE: 2616
TN   5 16
DES
DES Remote site 1
TN   005 0 00 16
TYPE 2616
CDEN 8D
CUST 0
AOM  0
FDN
TGAR 1
LDN  NO
NCOS 0
SGRP 0
RNPG 0
SCI  0
SSU
XLST
 CLS  CTD FBD WTD LPR MTD FND HTD ADD HFD
      MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD DTA DRG1
      POD DSX VMD CMSD CCSD SWD LND CNDD
      CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
      ICDD CDMD LLCN MCTD CLBD AUTU
      GPUD DPUD DNDD CFXD ARHD CLTD ASCD
      CPFA CPTA ABDD CFHD FICD NAID BUZZ AHD
      DDGA NAMA
      DRDD EXR0
      USMD USRD ULAD RTDD RBDD RBHD PGND FLXD FTTC DNDY DNO3
```

Telephone type

MIG RLC slot and port numbers

TGAR must be configured to allow trunk access. Refer to your PBX documentation for more details.

DTA defines the port as a data port.

```
TOV 0  MINS
DTAO MCA
PSEL  DMDM
HUNT
PSDS  NO
TRAN  ASYN
PAR  SPACE
DTR  ON
DUP  FULL
HOT  OFF
AUT  ON
BAUD 9600
DCD  ON
PRM  KBD ON
VLL  OFF
MOD  YES
INT  OFF
CLK  OFF
KBD  ON
RTS  OFF
PLEV 02
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
DNDR 0
KEY  00 SCR 1234 0     MARP
     01
     02
     03
     04
     05
     06
     07
     08
     09
     10
     11
     12
     13
     14
     15
```

Network ports must be defined as MCA.

The number that the Remote Office 9150 unit needs to connect to the MIG RLC. It must be a DID number.

MIG RLC configuration

Introduction

This section shows the configuration settings for the MIG RLC. You can obtain a similar configuration printout by performing a configuration download while connected to the MIG RLC.

Note: Configuration settings are separated by commas (,).

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 359.

```
IPCFG 10.2.1.1,255.255.0.0,10.2.1.10,10.3.1.2,255.255.0.0
```

MIG RLC's IP address information:

- IP address
- Subnet mask
- IP gateway
- Management IP address
- Management subnet mask

```
APPMODCFG 0,NC,NC
APPMODCFG 1,E,G729,G729
APPMODCFG 2,NC,NC
APPMODCFG 3,NC,NC
APPMODCFG 4,NC,NC
APPMODCFG 5,NC,NC
APPMODCFG 6,NC,NC
APPMODCFG 7,NC,NC
```

DSP application module
(only module 1 is configured
in this case)

```
SYSCFG 1,HOST1
```

Unit ID and node name

```
RLCCFG E,E
ACCFG D

PORTCFG 0,1,0,2,2,D
PORTCFG 1,1,0,2,2,D
PORTCFG 2,1,0,2,2,D
PORTCFG 3,1,0,2,2,D
PORTCFG 4,1,0,2,2,D
PORTCFG 5,1,0,2,2,D
```

Ports configured as remote ports

```
PORTCFG 6,0
PORTCFG 7,0
PORTCFG 8,0
PORTCFG 9,0
PORTCFG 10,0
PORTCFG 11,0
PORTCFG 12,0
PORTCFG 13,0
PORTCFG 14,0
PORTCFG 15,0
```

Ports configured as local ports

```
PORTCFG 16,2,2,6065556987
PORTCFG 17,0
PORTCFG 18,0
PORTCFG 19,0
PORTCFG 20,0
PORTCFG 21,0
PORTCFG 22,0
PORTCFG 23,0
PORTCFG 24,0
PORTCFG 25,0
PORTCFG 26,0
PORTCFG 27,0
    .
    .
    .
PORTCFG 63,0
```

Port configured as network port

```
RUNITCFG 1,E,0,2,45,45,3,1234567890,0987654321,E,Y,10.1.1.2,
         E,16,D,16,10,Y,6065556987,D
RUNITCFG 2,D,0,0,2,1,1,D,D,D
RUNITCFG 3,D,0,0,2,1,1,D,D,D
RUNITCFG 4,D,0,0,2,1,1,D,D,D
RUNITCFG 5,D,0,0,2,1,1,D,D,D
RUNITCFG 6,D,0,0,2,1,1,D,D,D
RUNITCFG 7,D,0,0,2,1,1,D,D,D
RUNITCFG 8,D,0,0,2,1,1,D,D,D
RUNITCFG 9,D,0,0,2,1,1,D,D,D
RUNITCFG 10,D,0,0,2,1,1,D,D,D
```

Remote unit connection information (unit 1):

- remote unit number
- 9150’s unit ID
- security information (inbound and outbound security IDs)
- remote unit’s IP address
- network port
- PSTN number

```
ONOFFCFG 1,SUN,0 00:00
ONOFFCFG 1,MON,0 00:00
ONOFFCFG 1,TUE,0 00:00
ONOFFCFG 1,WED,0 00:00
ONOFFCFG 1,THU,0 00:00
ONOFFCFG 1,FRI,0 00:00
ONOFFCFG 1,SAT,0 00:00
ONOFFCFG 2,SUN,0 00:00
ONOFFCFG 2,MON,0 00:00
ONOFFCFG 2,TUE,0 00:00
ONOFFCFG 2,WED,0 00:00
ONOFFCFG 2,THU,0 00:00
ONOFFCFG 2,FRI,0 00:00
ONOFFCFG 2,SAT,0 00:00
ONOFFCFG 3,SUN,0 00:00
ONOFFCFG 3,MON,0 00:00
ONOFFCFG 3,TUE,0 00:00
ONOFFCFG 3,WED,0 00:00
ONOFFCFG 3,THU,0 00:00
ONOFFCFG 3,FRI,0 00:00
ONOFFCFG 3,SAT,0 00:00
ONOFFCFG 4,SUN,0 00:00
ONOFFCFG 4,MON,0 00:00
ONOFFCFG 4,TUE,0 00:00
ONOFFCFG 4,WED,0 00:00
ONOFFCFG 4,THU,0 00:00
ONOFFCFG 4,FRI,0 00:00
ONOFFCFG 4,SAT,0 00:00
ONOFFCFG 5,SUN,0 00:00
ONOFFCFG 5,MON,0 00:00
ONOFFCFG 5,TUE,0 00:00
ONOFFCFG 5,WED,0 00:00
ONOFFCFG 5,THU,0 00:00
ONOFFCFG 5,FRI,0 00:00
ONOFFCFG 5,SAT,0 00:00
ONOFFCFG 6,SUN,0 00:00
ONOFFCFG 6,MON,0 00:00
ONOFFCFG 6,TUE,0 00:00
ONOFFCFG 6,WED,0 00:00
ONOFFCFG 6,THU,0 00:00
ONOFFCFG 6,FRI,0 00:00
```

Online/offline schedule

```
ONOFFCFG 6,SAT,0 00:00
ONOFFCFG 7,SUN,0 00:00
ONOFFCFG 7,MON,0 00:00
ONOFFCFG 7,TUE,0 00:00
ONOFFCFG 7,WED,0 00:00
ONOFFCFG 7,THU,0 00:00
ONOFFCFG 7,FRI,0 00:00
ONOFFCFG 7,SAT,0 00:00
ONOFFCFG 8,SUN,0 00:00
ONOFFCFG 8,MON,0 00:00
ONOFFCFG 8,TUE,0 00:00
ONOFFCFG 8,WED,0 00:00
ONOFFCFG 8,THU,0 00:00
ONOFFCFG 8,FRI,0 00:00
ONOFFCFG 8,SAT,0 00:00
ONOFFCFG 9,SUN,0 00:00
ONOFFCFG 9,MON,0 00:00
ONOFFCFG 9,TUE,0 00:00
ONOFFCFG 9,WED,0 00:00
ONOFFCFG 9,THU,0 00:00
ONOFFCFG 9,FRI,0 00:00
ONOFFCFG 9,SAT,0 00:00
ONOFFCFG 10,SUN,0 00:00
ONOFFCFG 10,MON,0 00:00
ONOFFCFG 10,TUE,0 00:00
ONOFFCFG 10,WED,0 00:00
ONOFFCFG 10,THU,0 00:00
ONOFFCFG 10,FRI,0 00:00
ONOFFCFG 10,SAT,0 00:00

FBQOSCFG 1,E,5,6,5,10,10,32
FBQOSCFG 2,D,5,6,5,10,10,32
FBQOSCFG 3,D,5,6,5,10,10,32
FBQOSCFG 4,D,5,6,5,10,10,32
FBQOSCFG 5,D,5,6,5,10,10,32
FBQOSCFG 6,D,5,6,5,10,10,32
FBQOSCFG 7,D,5,6,5,10,10,32
FBQOSCFG 8,D,5,6,5,10,10,32
FBQOSCFG 9,D,5,6,5,10,10,32
FBQOSCFG 10,D,5,6,5,10,10,32
```

Quality of Service settings (these are default settings)

```
Item not Configured
```

Caller ID (not configured; one line for each remote unit)

Remote Office 9150 unit

Introduction

This section shows the configuration settings for the Remote Office 9150 unit. You can obtain a similar configuration printout by performing a configuration download while connected to the Remote Office 9150 unit.

Note: Configuration settings are separated by commas (,).

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 359.

```
IPCFG 10.1.1.2,255.255.0.0,10.1.1.10
```

9150 unit's IP interface information:

- IP address
- Subnet mask
- IP gateway

```
APPMODCFG 0,SPARE,TSIDSP
APPMODCFG 1,E,G729,G729
APPMODCFG 2,NC,NC
APPMODCFG 3,NC,NC
APPMODCFG 4,1,1,E,1,1,5556987,60655569870101,E,1,1,
          5556988,60655569880101

APPMODCFG 5,NC,NC
APPMODCFG 6,NC,NC
APPMODCFG 7,NC,NC
```

On-board DSP module (module 0) and installed DSP application module (module 1)

ISDN BRI module configuration

- module number
- PSTN number for each B-channel
- SPID for each B-channel

```
SYSCFG 2, Remote site 1
```

Unit ID and node name

```
ROUCFG 13:00,0,JAN-13-2000,911,#222,#333,#345,#456,E
ACCFG N
```

System configuration:

- Emergency service number
- System date and time
- SPRE codes

```
RLCDETCFG 1,3,0987654321,1234567890,E,10.2.1.1,E,6135551234,E,D
```

Host PBX connection information:

- MIG RLC's unit ID
- security information (inbound and outbound security IDs)
- MIG RLC's IP address
- MIG RLC PSTN number

```
ROUDEVCFG 0,2,0,E,E,E,Bryan Dion,8734,04
ROUDEVCFG 1,2,1,E,E,E,Marc Horman,8707,04
ROUDEVCFG 2,2,2,E,E,E,Brad McAllister,8708,04
ROUDEVCFG 3,2,3,E,E,E,Andrew Wong,8760,04
ROUDEVCFG 4,2,4,E,E,E,Corey Smith,8709,04
ROUDEVCFG 5,2,5,E,E,E,Tracey Black,8743,04
ROUDEVCFG 6,0,E,E,E,John Brown,8611,04
ROUDEVCFG 7,1,0
ROUDEVCFG 8,1,0
ROUDEVCFG 9,1,0
ROUDEVCFG 10,1,0
ROUDEVCFG 11,1,0
ROUDEVCFG 12,1,0
ROUDEVCFG 13,1,0
ROUDEVCFG 14,1,0
ROUDEVCFG 15,1,0
ROUDEVCFG 16,1,0
ROUDEVCFG 17,1,0
ROUDEVCFG 18,1,0
ROUDEVCFG 19,1,0
ROUDEVCFG 20,1,0
ROUDEVCFG 21,1,0
ROUDEVCFG 22,1,0
ROUDEVCFG 23,1,0
ROUDEVCFG 24,1,0
ROUDEVCFG 25,1,0
ROUDEVCFG 26,1,0
ROUDEVCFG 27,1,0
ROUDEVCFG 28,1,0
ROUDEVCFG 29,1,0
ROUDEVCFG 30,1,0
ROUDEVCFG 31,1,0
ROUDEVCFG 32,2,31,E,E,E,FAX,8664,900
```

Port (station) configuration:

- Port number
- Local and remote capability
- CPND
- DN
- Restricted digits

Unconfigured ports
Note: The default capability is Remote.

Fax port configuration:

- Port number
- Local and remote capability
- CPND
- DN
- Restricted digits

```
FKEYCFG 0,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 1,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 2,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 3,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 4,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 5,2 TRN 12345678,3 CFW 4000,8 LC1 ,9 LC2 ,NC
FKEYCFG 6,8 LC1 ,9 LC2 ,NC
FKEYCFG 7,NC
FKEYCFG 8,NC
FKEYCFG 9,NC
FKEYCFG 10,NC
FKEYCFG 11,NC
FKEYCFG 12,NC
FKEYCFG 13,NC
FKEYCFG 14,NC
FKEYCFG 15,NC
FKEYCFG 16,NC
FKEYCFG 17,NC
FKEYCFG 18,NC
FKEYCFG 19,NC
FKEYCFG 20,NC
FKEYCFG 21,NC
FKEYCFG 22,NC
FKEYCFG 23,NC
FKEYCFG 24,NC
FKEYCFG 25,NC
FKEYCFG 26,NC
FKEYCFG 27,NC
FKEYCFG 28,NC
FKEYCFG 29,NC
FKEYCFG 30,NC
FKEYCFG 31,NC
FKEYCFG 32,NC
```

Local station feature keys configuration:

- Port number
- Feature key number
- Feature name
- DN (if applicable)
- locations of local call appearance keys 1 and 2

Trunk group configuration:

- Trunk group number
- Trunk access code
- B-channels (ISDN module and B-channel number)
- DNs to alert

```
TRKGRPCFG 1,E,#61,4.0.0 4.0.1,8739
TRKGRPCFG 2,D,#62,1.0.0 1.0.1 2.0.0 2.0.1,4002
TRKGRPCFG 3,D,#63,1.0.0 1.0.1 2.0.0 2.0.1,4004
TRKGRPCFG 4,D,#64,1.0.0 1.0.1 2.0.0 2.0.1,4006
TRKGRPCFG 5,D,#65,1.0.0 1.0.1 2.0.0 2.0.1,4008
TRKGRPCFG 6,D,#66,1.0.0 1.0.1 2.0.0 2.0.1,4010
TRKGRPCFG 7,D,#67,1.0.0 1.0.1 2.0.0 2.0.1,4012
TRKGRPCFG 8,D,#68,1.0.0 1.0.1 2.0.0 2.0.1,4014

Item not Configured
```

Caller ID (not configured)

Appendix D

Pin-out tables for RLC Multi-I/O cables

In this appendix

RLC Multi-I/O cable–Basic

Introduction

One RLC Multi-I/O cable–Basic (NTDR79AA) ships with each Meridian Internet Gateway Reach Line Card (MIG RLC). This cable provides the following connectivity:

- P1: the switch’s I/O panel
- P2: an external (user) Ethernet port
- P3: a serial port

If you lose your RLC Multi-I/O cable–Basic, contact your Nortel Networks distributor and request order number A0795280 to purchase a new one.

Pin-out information

The following table shows the pin-out of the RLC Multi-I/O cable–Basic:

Pair	Bundle	Wire color	From pin	To pin	Signal
1	W1	RED	P1-21	P2-5	EN0RXD+
1	W1	BLK	P1-46	P2-12	EN0RXD-
2	W1	WHT	P1-22	P2-6	EN0TXD+
2	W1	BLK	P1-47	P2-13	EN0TXD-
				P2-4	GND (SHD)
1	W2	RED	P1-17	P3-3	MMIRXD
1	W2	BLK	P1-42	P3-2	MMITXD
2	W2	WHT	P1-45	P3-5	GND
2					

Pair	Bundle	Wire color	From pin	To pin	Signal
			P3-1	P3-4	MMIDTR-MMIDCD
			P3-4	P3-6	MMIDTR-MMIDSR
			P3-7	P3-8	MMIRTS-MMICTS

RLC Multi-I/O cable–Enhanced

Introduction

The RLC Multi-I/O cable–Enhanced (NTDR80AA) is a 6-plug cable that provides the following connectivity:

- P1: the switch’s I/O panel
- P2: an external (user) Ethernet port
- P3: a serial port
- P4: the switch’s internal Ethernet port
- P5: the cross-connect to local telephones
- P6: a Frame Relay Access Device (FRAD)

You must order this cable separately by contacting your Nortel Networks distributor and requesting order code A0795281.

Pin-out information

The following table shows the pin-out of the RLC Multi-I/O cable–Enhanced:

Pair	Bundle	Wire color	From pin	To pin	Signal
1	W1	BLK	P1-21	P2-5	EN0RXD+
1	W1	RED	P1-46	P2-12	EN0RXD-
2	W1	BLK	P1-22	P2-6	EN0TXD+
2	W1	WHT	P1-47	P2-13	EN0TXD-
				P2-4	GND (SHD)
1	W2	BLK	P1-17	P3-3	SDIRXD
1	W2	RED	P1-42	P3-2	SDITXD
2	W2	BLK	P1-45	P3-5	GND

Pair	Bundle	Wire color	From pin	To pin	Signal
2	W2	WHT			
			P3-1	P3-4	SDIDTR-SDIDCD
			P3-4	P3-6	SDIDTR-SDIDSR
			P3-7	P3-8	SDIRTS-SDICTS
1	W3	BLK	P1-23	P4-5	EN1RXD+
1	W3	RED	P1-48	P4-12	EN1RXD-
2	W3	BLK	P1-24	P4-6	EN1TXD+
2	W3	WHT	P1-49	P4-13	EN1TXD-
1	W4	BLK	P1-1	P5-1	TCMR00
1	W4	RED	P1-26	P5-26	TCMT00
2	W4	BLK	P1-2	P5-2	TCMR01
2	W4	WHT	P1-27	P5-27	TCMT01
3	W4	BLK	P1-3	P5-3	TCMR02
3	W4	GRN	P1-28	P5-28	TCMT02
4	W4	BLK	P1-4	P5-4	TCMR03
4	W4	BLU	P1-29	P5-29	TCMT03
5	W4	BLK	P1-5	P5-5	TCMR04
5	W4	YEL	P1-30	P5-30	TCMT04
6	W4	BLK	P1-6	P5-6	TCMR05
6	W4	BRN	P1-31	P5-31	TCMT05
7	W4	BLK	P1-7	P5-7	TCMR06
7	W4	ORG	P1-32	P5-32	TCMT06

Pair	Bundle	Wire color	From pin	To pin	Signal
8	W4	RED	P1-8	P5-8	TCMR07
8	W4	WHT	P1-33	P5-33	TCMT07
9	W4	RED	P1-9	P5-9	TCMR08
9	W4	GRN	P1-34	P5-34	TCMT08
10	W4	RED	P1-10	P5-10	TCMR09
10	W4	BLU	P1-35	P5-35	TCMT09
11	W4	RED	P1-11	P5-11	TCMR10
11	W4	YEL	P1-36	P5-36	TCMT10
12	W4	RED	P1-12	P5-12	TCMR11
12	W4	BRN	P1-37	P5-37	TCMT11
13	W4	RED	P1-13	P5-13	TCMR12
13	W4	ORG	P1-38	P5-38	TCMT12
14	W4	GRN	P1-14	P5-14	TCMR13
14	W4	WHT	P1-39	P5-39	TCMT13
15	W4	GRN	P1-15	P5-15	TCMR14
15	W4	BLU	P1-40	P5-40	TCMT14
16	W4	GRN	P1-16	P5-16	TCMR15
16	W4	YEL	P1-41	P5-41	TCMT15
1	W5	BLK	P5-9	P6-2	V35TXDA
1	W5	RED	P5-34	P6-14	V35TXDB
2	W5	BLK	P5-10	P6-3	V35RXDA
2	W5	WHT	P5-35	P6-16	V35RXDB

Pair	Bundle	Wire color	From pin	To pin	Signal
3	W5	BLK	P5-11	P6-4	V35RTS
3	W5	GRN	P5-36	P6-5	V35CTS
4	W5	BLK	P5-12	P6-20	V35DTR
4	W5	BLU	P5-37	P6-6	V35DSR
5	W5	BLK	P5-13	P6-8	V35DCD
5	W5	YEL	P5-38	P6-7	V35GND
6	W5	BLK	P5-14	P6-17	V35RXCA
6	W5	BRN	P5-39	P6-9	V35RXCB
7	W5	BLK	P5-15	P6-24	V35TXCA
7	W5	ORG	P5-40	P6-11	V35TXCB
8	W5	RED	P5-16	P6-15	V35TXTA
8	W5	WHT	P5-41	P6-12	V35TXTB

Appendix E

Safety and regulatory information

In this appendix

Overview

Introduction

The MIG RLC complies with a variety of regulatory standards and classifications. This section contains these international criteria.

International safety compliance

This appendix is a brief listing of the MIG RLC’s compliance with the following safety standards:

- Underwriters Laboratory (UL)
- Canadian Standards Association (CSA)
- Europe
- Australia

Electromagnetic compatibility

The MIG RLC does not interfere with the operation of other licensed communications systems according to the standards set forth by Australia, the United States, and Canada.

Electromagnetic immunity

The MIG RLC in a Meridian 1 system resists electromagnetic interference.

Electrostatic discharge

The MIG RLC is immune to electrostatic discharges typical for an office environment (carpeted floors, low humidity) according to the test method specified by IEC 1000-4-2.

International safety compliance

Underwriters Laboratory (UL)

The Meridian Internet Gateway Reach Line Card complies with and is listed under UL 1950, second edition.

Canadian Standards Association (CSA)

The Meridian Internet Gateway Reach Line Card complies with and is listed under CSA C22.2, No. 950.

Europe

The Meridian Internet Gateway Reach Line Card complies with and is listed under EN90650.

Australia

Meridian Internet Gateway Reach Line Card complies with and is listed under TS001\AS 3260.

Electromagnetic compatibility

Introduction

The MIG RLC does not interfere with the operation of other licensed communications systems according to the standards set forth by Australia, the United States, and Canada.

Details

The MIG RLC does not adversely impact the compliance of the Meridian 1 system to

- AS 3548 Class B (Australia)
- Class A of FCC Part 15, Subpart J
- CSPR B requirements

The margin is 2 dB better than the specified limit.

Electromagnetic immunity

Introduction

The MIG RLC in a Meridian 1 system resists electromagnetic interference.

Details

It performs correctly when subjected to narrow band radiated fields in frequency range 500 kHz to 1 GHz (field strength up to 10 V/m, 1 kHz, 50% modulated AM signal) per IEC 1000-4-3.

Electrostatic discharge

Introduction

The MIG RLC is immune to electrostatic discharges typical for an office environment (carpeted floors, low humidity) according to the test method specified by IEC 1000-4-2.

Details

No damage or malfunction occurs at up to +/-8kV of direct discharge. An indirect discharge of up to +/-16 kV does not result in malfunction of the system (to adjacent equipment or connected cabling).

The requirements for both “closed door” and “open door” have been met.

Glossary

10BaseT Ethernet

The Ethernet standard for baseband local area networks using twisted-pair cable carrying 10 megabits per second (Mbps) in a star topology.

A

A-law

A companding technique used in encoding and decoding audio signals in 30-channel pulse code modulated (PCM) systems. A-law companding is the primary method used in Europe. *See also* Mu-law.

adapter

Hardware required to support a particular device. For example, network adapters provide a port for the network wire. Adapters can be expansion boards or part of the computer's main circuitry.

administrator

A user who is responsible for maintaining the MIG RLC or its associated remote units.

agent

A person who is responsible for handling customer calls.

analog

The type of signal used by most telephone connections. A modem converts a digital (computer) signal to analog, and vice versa, so that the signal can travel through telephone lines.

API

See application program interface.

application

A program that runs on a computer.

application program interface

A set of routines, protocols, and tools that programmers use to develop software applications. APIs simplify the development process by providing commonly used programming procedures.

Automatic Call Distribution (ACD) applications

A separate system or built-in feature of a PBX that equally distributes incoming calls to agents. As calls come in, they are placed into a queue (or a waiting line) for the next available agent. The MIG RLC and its associated remote units support all of Nortel Networks' ACD applications.

B

bandwidth

The amount of data that the network can transmit, usually expressed in Mbytes per second.

baseboard

See motherboard.

Basic Input/Output System

Flash ROM-based code that runs the Power-On Self-Test (POST) and bootstrap loader. BIOS contains low-level access routines for hardware that can be called from DOS.

BIOS

See Basic Input/Output System.

bit

Short for binary digit, the smallest unit of information on a machine. A single bit can hold only one of two values: 0 or 1.

branch station

A phoneset or fax machine located at the Remote Office 9150 site.

BRI

Basic Rate Interface. An ISDN subscriber service that uses two B (64 Kbps) channels and one D (64 Kbps) channel to transmit voice, video, and data signals.

bridge

A protocol-independent device that connects two LANs or two segments of the same LAN. Bridges are faster (and less versatile) than routers because they forward packets without analyzing and rerouting messages.

bus

A collection of wires that connects the microprocessor and main memory to internal computer components. All buses consist of an address bus that transfers data and a data bus that transfers information about where the data should go.

In a network, the bus (also called the backbone) is the main cable that connects all devices on a LAN.

byte

Abbreviation for binary term, a unit of storage capable of holding a single character. On almost all modern computers, a byte is equal to eight bits. Large amounts of memory are indicated in terms of kilobytes (1024 bytes), megabytes (1 048 576 bytes), and gigabytes (1 073 741 824 bytes).

C

cache

A temporary storage area in computer memory.

call duration timer

Used in circuit-switched mode only, it specifies the minimum length of time that each call to the host PBX remains open, regardless of telephone activity (or lack thereof).

call on demand

A call connection that is opened only when a connection to the host PBX is required. This is different from a permanent connection, which is open all the time.

call treatment

A method of handling applied to a call while it is waiting to be answered or serviced.

Caller ID

Caller ID is used on the MIG RLC to identify the number of the caller requesting access to one of its ports. It is also used on the Remote Office 9150 unit to authenticate incoming calls from the MIG RLC.

Calling Line Identification

An optional service that identifies the telephone number of the caller. This information can then be used to route the call to the appropriate agent or skillset. The caller's telephone number can also be displayed on a phoneset.

card

A thin, rectangular plate on which chips and other electronic components are placed. Examples of cards include motherboards, expansion boards, daughterboards, controller boards, network interface cards, and video adapters.

CD-ROM

A type of optical disk capable of storing large amounts of data (up to 1 Gbyte), although the most common size is 630 Mbytes. A single CD-ROM has the storage capacity of 700 floppy disks and is particularly well-suited to information that requires large storage capacity.

CLAN

See Customer local area network.

CLID

See Calling Line Identification.

client

The part of a client/server architecture that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.

codec

An acronym for COder-DECoder. A device that codes analog signals into digital signals for transmission and decodes digital signals into analog signals for receiving.

COM or COMM

Communications port. This usually refers to the Logical Device name of PC serial ports as defined by DOS.

computer-based training

Computer-based training (CBT) is a type of education in which students learn by running special training programs on a computer. CBT is especially effective for training people to use computer applications, because the CBT program can be integrated with the applications.

Configuration Manager

The software application used to configure and administer the Remote Office 9150 unit and the MIG RLC to which it is connected.

controller board

A special type of expansion board that contains a controller for a peripheral device. When you attach new devices to a computer, such as a disk drive, often a controller board must also be added.

CPU

Central processing unit. This is the system unit that holds a PC's essential components.

crash

A serious computer failure during which the computer stops working or a program closes unexpectedly. A crash indicates a hardware malfunction or a serious software bug.

Customer local area network

The LAN to which your corporate services and resources connect. The MIG RLC and its associated remote units both connect to the CLAN.

D

daughterboard

Usually used as a synonym for an expansion board, a daughterboard is any printed circuit board that connects directly or indirectly to a motherboard.

DB-9 connector

A 9-pin connector labeled ADMIN that provides the RS-232 serial port interface. This serial port connection can be used to configure a Remote Office 9150 unit that is directly connected to a PC.

DB-25 connector

A 25-pin connector labeled V.35 provides a V.35 serial port connection for voice and signaling. This connection can be used to send voice traffic over a Frame Relay network instead of an Ethernet network.

Note: On the MIG RLC and Remote Office 9150 unit, the V.35 connector is for future use.

DHCP

See dynamic host configuration protocol.

digital signal processor

A special type of coprocessor that manipulates analog data, such as sound or photographs, that has been converted to digital form.

directory number

The number that identifies a phoneset on a switch. The directory number (DN) could be a local extension (local DN), a public network telephone number, or an automatic call distribution directory number (ACD-DN).

DLL

See dynamic link library.

DN

See directory number.

driver

A program that controls a device. Every device, whether it is a printer, disk drive, or keyboard, must have a driver program. A driver acts like a translator between the device and programs that use the device.

DSP

See digital signal processor.

dynamic host configuration protocol

A protocol for dynamically assigning IP addresses to devices on a network.

dynamic link library

A library of executable functions or data that can be used by a Windows application. Typically, a DLL provides one or more particular functions and a program accesses the functions by creating either a static or dynamic link to the DLL. A DLL can be used by several applications at the same time.

dynamic port pool

A MIG RLC feature that is similar to multiuser ports in that multiple stations can share ports on the MIG RLC. However, users sharing ports from a dynamic pool are assigned to the first available port on the MIG RLC.

E

ECC

See error correction code.

EEPROM

See electronically erasable programmable read-only media.

ELAN

See embedded local area network.

electronically erasable programmable read-only media

A memory chip that needs only a higher than normal voltage and current to erase its contents. An EEPROM chip can be erased and reprogrammed without taking it out of its socket. An EEPROM chip gives a computer and its peripherals a means of storing data without the need for a constant supply of electricity.

embedded local area network

This is the network connection from the PBX to the MIG RLC. It is an Ethernet LAN that is segmented from the rest of the Ethernet network and enables signaling and administration access to the MIG RLC. Nortel Networks recommends the following:

- IP traffic should not be routed between the main network and the ELAN.
- An IP route should not be established between the two LANs.

Emergency Service Number

The Remote Office 9150 unit allows you to program an emergency service number (such as 911).

EMI

Electromagnetic interference

error correction code

A scheme that can detect and fix single-bit memory errors without crashing the system. Also known as Error Detection and Correction (EDAC).

Ethernet

A widely used LAN protocol that uses a bus topology and supports data transfer rates of 10 Mbps.

event

An occurrence or action on the MIG RLC or remote unit, such as the sending or receiving of a message, the opening or closing of an application, or the reporting of an error. Some events are for information only, while others can indicate a problem.

expansion board

Any board that plugs in to one of the computer’s expansion slots. Expansion boards include controller boards, LAN cards, and video adapters.

expansion bus

Enables expansion boards to access the microprocessor and memory. *See also* bus.

F

first-level threshold

The value that represents the lowest value of the normal range for a given field in a threshold class. The system tracks how often the value for the field falls below this value.

G

G.711

G.711 is the international standard for encoding telephone audio on a 64 Kbps channel. It is a pulse code modulation (PCM) scheme operating at an 8 kHz sample rate, with 8 bits per sample. According to the Nyquist theorem, which states that a signal must be sampled at twice its highest frequency component, G.711 can encode frequencies between 0 and 4 kHz. Telcos can select between two different variants of G.711: A-law and mμ-law. A-law is the standard for international circuits.

G.726

G.726 is a standard ADPCM algorithm specified by the International Telecommunication Union (ITU) for reducing the 64 kbps A-Law or mμ-law logarithmic data of a normal telephone line to 16, 24, 32, or 40 kbps.

G.729

G.729 is a voice compression International Telecommunications Union (ITU) standard that can be used in a wide range of applications including wireless communications, digital satellite systems, packetized speech, and digital leased lines. G.729 provides 8 Kbps of bandwidth for compressed speech at toll quality (equivalent to G.726 32 Kbps ADPCM under clean channel condition).

gateway

A device that functions as a node on two or more networks, forwarding packets from one network to addresses in the other networks. In Remote Office context, the gateway is the device on the network that directs traffic to and from the Remote Office 9150 unit or MIG RLC.

Gbyte

1 073 741 824 bytes. One Gbyte is equal to 1024 Mbytes.

general protection fault

A computer condition that causes a Windows application to crash. GPFs usually occur when one application attempts to use memory assigned to another application.

GPCP

General purpose computing platform

GPF

See general protection fault.

graphical user interface

The information displayed on the monitor when a Windows application (or another non-command-based application) runs. A graphical user interface uses features such as pointers, icons, I-beams, and menus to make the program easier to use.

H

handshaking

A process involved in establishing a valid connection or signal between two pieces of hardware or communications software.

host call appearance key

An assigned key on the telephone set at the remote site that is used to establish a connection with the host PBX or to receive incoming calls from the host PBX.

host-controlled call mode

When a call is placed to someone at the host site, or when someone from the host site calls the remote site, the call is in host-controlled call mode. Calls in host-controlled mode are routed through the PBX.

host station

A telephone set located at the host PBX site.

host trunk

The ISDN PRI or TI connection located at the host site. Host trunks are used to route calls from the host PBX to remote sites over the circuit-switched network.

hub

A common connection point for all 10Base-T cables connected to a small network. A hub enables data to go from one device to another.

I

icon

A small picture that represents an object or program in a graphical user interface.

idle timer

Identifies the maximum length of time during which an ISDN connection should remain idle before it can be closed. Idle means that a voice connection does not exist, and buttons are not being pressed on the digital telephone.

input/output

Refers to any operation, program, or device that enters data into a computer or extracts data from a computer.

I/O

See input/output.

IP

Internet Protocol. The protocol within TCP/IP that governs the breakup of data messages into packets, the routing of the packets from sender to destination network, and the reassembly of the packets into the original data messages at the destination.

IP address

Internet Protocol address. An identifier for a computer or device on a TCP/IP network. Networks use the TCP/IP protocol to route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be 0–255. For example, 1.160.10.240 can be an IP address.

ISDN

Integrated Services Digital Network. A worldwide digital communication protocol that permits telephone networks to carry data, voice, and other source material. There are two kinds of ISDN lines—Primary Rate Interface (PRI) and Basic Rate Interface (BRI). *See also* BRI.

J

jumper

A metal bridge that closes an electrical circuit. Typically, a jumper consists of a plastic plug that fits over a pair of protruding pins. Jumpers are sometimes used to configure expansion boards. By placing a jumper plug over a different set of pins, you can change a board’s parameters.

K

kbyte

1024 bytes

L

LAN

See Local area network.

LED

Light emitting diode

Local area network

A computer network that spans a relatively small area. Most LANs connect workstations and personal computers and are confined to a single building or group of buildings.

local call

A call that originates at your site.

local call appearance key

An assigned key on the telephone set at the Remote Office 9150 site that is used to call another station at the branch office, or to make and receive calls through the local PSTN.

local-controlled call mode

When you place a call from a specified local call appearance key, or your call is to another telephone at your branch site, you are in local-controlled call mode. Calls in local-controlled mode are routed through the local PSTN.

local station

A telephone set located at the Remote Office 9150 site.

M

M1

Meridian 1 PBX

MAT

Meridian Administration Tools. This is a Nortel Networks software application that is used to administer the Meridian 1 PBX.

Mbyte

1 048 576 bytes

megahertz

One million cycles per second.

MHz

See megahertz.

MIG RLC

An abbreviation for Meridian Internet Gateway Reach Line Card. The MIG RLC is installed on the Meridian 1 PBX at the host location and relays voice and signaling information from the digital telephones connected at a remote site to the Meridian 1 PBX at the host site.

motherboard

The principal board that has connectors for attaching devices to the bus. Typically, the motherboard contains the CPU, memory, and basic controllers for the system. On PCs, the motherboard is often called the system board.

MTBF

Mean time between failures

Mu-law

A companding method for encoding and decoding audio signals in 24-channel pulse-code-modulated (PCM) systems. Mu-law is the method used in North America and Japan. *See also* A-law.

Multiuser ports

A MIG RLC port feature that allows multiple stations to time-share a single port on the host PBX. All stations that use a multiuser port are always assigned to the same port number (TN) on the host PBX.

N

network interface card

An expansion board that enables a PC to be connected to a local area network (LAN).

NIC

See network interface card.

node

A device connected to the network capable of connecting to other network devices. For example, the MIG RLC and Remote Office 9150 unit are both nodes on the network.

NPA

See Number Plan Area.

Number Plan Area

Area code

NVRAM

Non-Volatile Random Access Memory

O

OA&M

Operations, administration, and maintenance

object linking and embedding

A compound document standard that enables you to create objects with one application and then link or embed them in a second application.

OEM

Original equipment manufacturer

online/offline table

The online/offline table is configured on the MIG RLC. It allows you to schedule times that the host PBX connection is made available to the remote site and at which times all telephones at the remote site can use only the local telephone service.

The online/offline table is used for controlling ISDN BRI costs.

Open System Interconnection

A worldwide communications standard that defines a framework for implementing protocols in seven layers.

OS

Operating Standard

OSI

See Open System Interconnection.

P

packetized voice

Digital Signal Processors (DSPs), located in the Remote Office 9150 unit and MIG RLC, convert analog voice into digital data. The data is constructed as a UDP/IP voice packet for transmission over an IP network.

parity

The quality of being either odd or even. The fact that all numbers have parity is commonly used in data communications to ensure the validity of data.

PBX

See private branch exchange.

pegging

The action of incrementing statistical counters to track system events.

pegging threshold

A threshold used to define a cut-off value for statistics such as short call and service level. Pegging thresholds are used in reports and historical statistics.

personal directory number

A DN on which an agent can be reached directly, usually for private calls.

ping

Packet Internet Groper. A protocol that can be used to test the Ethernet connection to devices on the network (such as the MIG RLC and its associated remote units).

POST

See Power-On Self-Test.

Power-On Self-Test

Initializes and performs rudimentary tests on baseboard hardware, including CPU, floating point unit, interrupts, memory, real-time clock, video, and auto-initializing PCI and EISA bus.

priority DN

A user station can be configured as a priority DN. There are two levels of priority—high and normal. High priority level allows you to

- ensure a trunk is always available
- use PSTN trunking for the host PBX connections
- move the high priority DN first from the IP network to the PSTN

private branch exchange

A telephone switch, typically used by a business to service its internal telephone needs. A PBX usually offers more advanced features than are generally available on the public network. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX.

protocol

A standard format used for communication between two devices. The protocol determines the type of error checking to be used, the data compression method (if any), how the sending device will indicate that it has finished sending a message, and how the receiving device will indicate that it has received a message.

PSTN

Public Switched Telephone Network (also known as the public telephone network).

Q

QoS transitioning technology

Technology that can automatically switch calls from the IP network to the circuit-switched network when the voice Quality of Service falls below a predetermined threshold, and back to the IP network when the Quality of Service returns to normal.

R

RAM

Random Access Memory. This is the most common type of memory found in computers and other devices, such as printers. The term RAM is usually synonymous with main memory, the memory available to programs. For example, a computer with 8 Mbytes of RAM has approximately 8 million bytes of memory that programs can use.

remote station

A phoneset or fax machine located at the Remote Office 9150 site.

remote trunk

From the MIG RLC’s point of view, remote trunks are the ISDN BRI connections between the PSTN and the Remote Office 9150 unit located at the branch office site.

RJ-45 connector

An 8-position, 8-conductor modular jack that provides the 10BaseT Ethernet connection.

ROM

Read-Only Memory. This is the computer memory on which data has been prerecorded and from which it cannot be removed.

router

A device that connects two LANs. Routers are similar to bridges but provide additional functionality, such as the ability to filter messages and forward them to different places based on various criteria.

S

second-level threshold

The value used in display thresholds that represents the highest value of the normal range for a given statistic.

security identifier

The remote unit sends the branch office security identifier (password) to the MIG RLC for each connection request. The MIG RLC matches the identifier configured for the MIG RLC port. When it finds a match, it grants access to the port and allows the call to proceed.

serial port

A general-purpose interface that can be used for almost any type of device, including modems, mice, and printers (although most printers are connected to a parallel port). Most serial ports on personal computers conform to the RS-232C or RS-422 standards.

server

A computer or device on a network that manages network resources. Examples of servers include file servers, print servers, network servers, and database servers.

service

A process that adheres to a Windows NT structure and requirements. A service provides system functionality.

Service Control Manager

A Windows NT process that manages the different services on the PC.

silence suppression

A feature that prevents packet transmission during periods when there is no voice data present.

Simple Network Management Protocol

A set of protocols for managing complex networks. SNMP sends messages, called protocol data units (PDUs) to different parts of a network, and then analyzes the responses.

single-user ports

A MIG RLC port that supports one remote station.

SNMP

See Simple Network Management Protocol.

SPID

Service Profile Identifier

SPRE code

A Special Prefix code that is used to initiate use of a PBX feature. In a Remote Office context, SPRE codes are used to

- toggle a remote site between online and offline modes
- use the paging feature
- switch an analog or ATA-equipped station from host-controlled mode to local-controlled mode so that local calls can be made
- register a Remote Office 9150 unit for a multiuser or dynamic port

station

A phoneset or fax machine located at a Remote Office 9150 site.

stop bit

In asynchronous communications, a bit that indicates a byte has just been transmitted. Every byte of data is preceded by a start bit and followed by a stop bit.

subnet mask

A subnet mask is the part of the IP address used to represent a subnetwork within a network. A typical IP address might be 192.210.34.144. Each part of this address is made up of eight bits. The subnet mask identifies to the MIG RLC or remote unit what portion of the IP address represents the network (and subnetwork) and what portion represents the host.

switch

In a telecommunications network, a switch is the hardware that receives phone calls and provides connections to phonesets. The switch allows a connection to be established as necessary and terminated when there is no longer a session to support it.

In networks, a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) of the OSI Reference Model and, therefore, support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.

switch resource

A device that is configured on the switch.

T

TCP/IP

Transport Control Protocol/Internet Protocol. The communication protocol used to connect devices on the Internet. TCP/IP is the standard for transmitting data over networks.

threshold

A value for a statistic at which system handling of the statistic changes.

threshold class

A set of options that specifies how statistics are treated in reports and real-time displays. *See also* pegging threshold.

trunk

A communications link between a PBX and the public central office, or between PBXs. Various trunk types provide services such as Direct Inward Dialing (DID), ISDN, and central office connectivity.

trunk access code

A trunk access code is a number that is used by the Remote Office 9150 unit to determine which trunk to use when routing a call. For example, 9 is a common trunk access code used to obtain an outside line.

Note: All trunk access codes are configured on the Remote Office 9150 unit with a pound sign (# in North America) so that there are no conflicts with host PBX numbering plans.

trunk groups

A trunk group consists of one or more trunk lines that are logically grouped. You can configure up to eight trunk groups on the Remote Office 9150 unit.

trunk interface modules

Used to route calls over the circuit-switched network. The number of modules you must install on the Remote Office 9150 unit depends on the number of simultaneous calls you want in host-controlled or local-controlled mode.

U

uninterruptible power supply

A power supply that includes a battery to maintain power in the event of a power outage. Typically, a UPS keeps a computer running for several minutes after a power outage, enabling you to save data that is in RAM and to shut down the computer safely.

UPS

See uninterruptible power supply.

utility

A program that performs a specific task, usually related to managing system resources. Operating systems contain a number of utilities for managing disk drives, printers, and other devices.

V

V.35

An ITU-T standard describing a synchronous, physical layer protocol used for communications between a network access device and a packet network. V.35 is most commonly used in the United States and in Europe, and is recommended for speeds up to 48 Kbps. In practice, V.35 is used for synchronous transmission up to 2.048 Mbps.

V.35 interface

The V.35 interface is for future use.

voice compression

Prior to transmission, the voice data is compressed; after transmission, the data is converted back to voice data at the destination. Voice compression means that voice consumes less bandwidth, leaving more bandwidth for data or other voice or fax communications.

voice jitter attenuation

A feature that removes the variable delays from the voice packets sent across the IP network, thus avoiding awkward-sounding speech.

Voice over IP (VoIP)

Technology that uses the IP data network to carry the voice conversation and telephone set control signals between a remote site and the host PBX.

W

WAN

Wide area network. A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs). The largest WAN in existence is the Internet.

Fields index

Index

NORTEL NETWORKS™

How the world shares ideas.

Reader Response Form

Product release 1.0
Meridian Internet Gateway Reach Line Card
Installation and Administration Guide
555-8421-210

Tell us about yourself:

Name: ______________________________

Company: ______________________________

Address: ______________________________

____

Occupation: ______________________ **Phone:** ______________

1. What is your level of experience with this product?

   □ New user □ Intermediate □ Experienced □ Programmer

2. How do you use this book?

   □ Learning □ Procedural □ Reference □ Problem solving

3. Did this book meet your needs?

   □ Yes □ No

   If you answered No to this question, please answer the following questions.

4. What chapters, sections, or procedures did you find hard to understand?

   ____

   ____

   ____

5. What information (if any) was missing from this book?

   ____

   ____

   ____

6. How could we improve this book?

   ____

   ____

   ____

Please return your comments by fax to (416) 597-7104, or mail your comments to
Toronto Information Products, Nortel Networks, 522 University Avenue, 14th Floor, Toronto, ON,
Canada, M5G 1W7.

NORTEL NETWORKS™

How the world shares ideas.

Reader Response Form

Meridian Internet Gateway

Reach Line Card

Installation and Administration Guide

Toronto Information Products
Nortel Networks
522 University Avenue, 14th Floor
Toronto, Ontario, Canada
M5G 1W7

Printed in the United States of America

All information contained in this document is subject to change without notice. Nortel Networks reserves the right to make changes to equipment design or program components, as progress in engineering, manufacturing methods, or other circumstances may warrant.

*Nortel Networks, the Nortel Networks logo, the Globemark, How the World Shares Ideas, and Unified Networks, Meridian 1, and SL-100 are trademarks of Nortel Networks.

PROCOMM PLUS is a trademark of Datastorm Technologies, a subsidiary of Quarterdeck Corporation.

HYPERTERMINAL is a trademark of Hilgraeve, Incorporated.

MICROSOFT, MS-DOS, WINDOWS, and WINDOWS NT are trademarks of Microsoft Corporation.

Product release:	1.0
Publication number:	555-8421-210
Document release:	Standard 1.0
Date:	March 2000

Printed in the United States of America

NORTEL NETWORKS™

How the world shares ideas.