555-8421-215

Remote Office 9150

Installation and Administration Guide

Product release 1.0 Standard 1.0 March 2000

NORTEL NETWORKS™

How the world shares ideas.

NTDR84AA

Remote Office 9150

Installation and Administration Guide

Product release:	1.0
Publication number:	555-8421-215
Document release:	Standard 1.0
Date:	March 2000

FCC: Customer instructions

The Remote Office 9150 unit complies with Part 68 of the FCC rules. On the bottom side of the equipment is a label that contains, among other information, the FCC registration number and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

The Remote Office 9150 unit uses the following standard connections and codes: USOC Code: RJ21X, Facility Interface Code: 02DU5-64, and Service Order Code: 6.0F.

The REN number shown on the label is used to determine the number of devices that can be connected to the telephone line. Excessive RENs on the telephone line can result in the devices not ringing in response to an incoming call. The sum of the RENs should not exceed five (5.0). To be certain of the number of devices that can be connected to a line, as determined by the total RENs, contact the local telephone company.

If the equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service might be required. However, if advance notice is not practical, the telephone company will notify you as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

No repairs can be performed by you. If you experience trouble with this equipment, please contact the following for repair and warranty information:

Nortel Networks
Product Service Center
640 Massman Drive. Nashville, TN 31210
Phone: 1-800-251-1758

If the equipment is causing harm to the telephone network, the telephone company might request that you disconnect the equipment until the problem is resolved.

This equipment cannot be used on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission, or corporation commission for information.

Industry Canada: Equipment attachment limitation

NOTICE: The Industry Canada Label identifies certified equipment. This certification means that the equipment meets telecommunications network protective, operational, and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee that the equipment will operate to the user's satisfaction.

Before installing this equipment, you should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. You should be aware that compliance with the above conditions might not prevent degradation in service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, can give the telecommunications company cause to request you to disconnect the equipment.

You should ensure, for your own protection, that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution can be particularly important in rural areas.

Caution: You should not attempt to make such connections yourself, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

NOTICE: The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface can consist of any combination of devices subject only to the requirements that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.

Publication history

March 2000

This is the Standard 1.0 issue of the *Remote Office 9150 Installation and Administration Guide* for Remote Office 9150 Release 1.0.

Contents

Preface

About this document

In this preface

About this guide

Introduction

The *Remote Office 9150 Installation and Administration Guide* describes how to install, configure, and manage the Remote Office 9150 unit in a branch office.

Who should read this guide

This guide is for the following individuals who are responsible for the installation, configuration, and day-to-day management of the Remote Office 9150 unit system:

- Nortel Networks distributors
- telecom network managers and administrators
- data network managers and administrators
- branch office managers and administrators

Assumptions

This document assumes that you have the skills listed on page xviii.

How to use this guide

This guide explains, step-by-step, how to install, configure, and use the Remote Office 9150 unit product. To get an overview of what you need to do, review this guide before beginning Remote Office 9150 unit installation and configuration.

When you are ready to begin, follow the steps in the order in which they are presented. This helps you to achieve a successful installation.

In this guide

Chapter 1, “Remote Office 9150 description”
This chapter describes the Remote Office 9150 system, how it works, and its features.

Chapter 2, “Planning for installation”
This chapter helps you to plan for Remote Office 9150 unit installation and configuration. This chapter includes topics such as

- choosing a suitable location
- issues to consider when incorporating the Remote Office 9150 unit product into your networks
- managing system resources
- planning network security
- planning user station configuration
- installation checklists
- methods for implementing the Remote Office 9150 unit into your network
- gathering information for configuration
- planning for future growth

Chapter 3, “Installing the Remote Office 9150 unit”
This chapter explains how to

- install and connect the Remote Office 9150 unit
- install or replace trunk interface and DSP application modules
- install and start the Configuration Manager software

Chapter 4, “Configuration Manager overview”
This chapter describes the Configuration Manager screens. It also describes the conventions used in this guide to present instructions for working with the screens.

Chapter 5, “Configuring the Remote Office 9150 unit”
This chapter explains how to use the Configuration Manager software to configure

- trunks used by the Remote Office 9150 unit
- connection information needed to establish connections between the MIG RLC on the host PBX and the Remote Office 9150 unit at the branch office
- user stations connected to the Remote Office 9150 unit

Chapter 6, “Using Remote Office 9150 stations”
This chapter describes digital telephone usage and features as they pertain to Remote Office 9150.

Chapter 7, “Administration”
This chapter describes how to perform periodic administration tasks, such as performing backups, restores, and upgrades, and viewing system logs and statistics.

Chapter 8, “Troubleshooting”
This chapter describes how to determine why the Remote Office 9150 and its connected telephones are not working.

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 Remote Office 9150 unit configuration
- determine what you need to expand the Remote Office 9150 unit’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, “Connection pin-out tables”
This section provides pin-out tables for each Remote Office 9150 unit connector.

Glossary
Many terms in this manual have meanings specific to the telecommunications and data networking fields, or specific to the Remote Office 9150 unit. You can find the definitions of terms used in this manual, as well as a few related terms.

Indexes
The Fields index helps you to locate information about the fields on the Configuration Manager screens. Use the index when you want to know the function of the field.

The main index provides an alternative 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 is helpful when working with the Remote Office 9150 unit:

- the Meridian 1 switch
- Meridian digital telephones

Telecommunications experience

Knowledge of, or experience with, telecommunications is helpful when working with the Remote Office 9150 unit:

- Extended Digital Line Cards (XDLCs) and how they work
- configuring voice and data ports
- configuring ISDN BRI, PRI (or other types of trunks)
- establishing telephone connections

Data networking experience

Knowledge of, or experience with, data networking is helpful when working with the Remote Office 9150 unit:

- networking fundamentals and concepts
- IP protocol
- network addressing and routing

- network traffic analysis and provisioning
- network security
- Voice over IP (general knowledge)

PC experience or knowledge

Knowledge of, or experience with, the following PC tasks is helpful when administering the Remote Office 9150 unit:

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

Other experience or knowledge

Other types of experience or knowledge that can be useful include the following:

- analytical skills
- troubleshooting skills

Related information products

Introduction

This section lists information products where you can find additional information.

Meridian 1 documents

The following documents describe how to establish telephone and trunk connections between the Remote Office 9150 unit and the BIX in-building cross-connect system:

- *Meridian 1 Installation planning* (NTP 553-3001-120)
- *Telephone and attendant console installation* (NTP 553-3001-215)
- *BIX* In-Building Cross-Connect System Material Installation and Servicing (Wall-Mounted System)* (NTP 631-4511-200)

Remote Office 9150 and MIG RLC documents

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

The *Release Notes* describe the features and known problems for the Meridian Internet Gateway Reach Line Card (MIG RLC) and Remote Office 9150 branch office system.

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

Meridian Internet Gateway Reach Line Card Installation and Administration Guide (NTP 555-8421-210)

This document, written for both the Meridian 1 installer and administrator, explains how to install and configure the Meridian Internet Gateway Reach Line Card on the Meridian 1 PBX.

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 Application 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 Remote Office 9150 unit:

- *Remote Office Product CD-ROM*, which contains
  - 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 administrators of Nortel Networks customers. The course explains how to install, configure, and manage the MIG RLC and Remote Office 9150 unit.

How to obtain the product 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. For more information, refer to the *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 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.

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 in a "Getting there" statement.

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)

Example

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 “Selecting the device type for offline configuration” on page 187.
you are performing an online configuration	connect to, and then log on to the node as described in “Logging on to a unit” on page 189.

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 Remote Office 9150 unit appears in the right pane.

Chapter 1

Remote Office 9150 description

In this chapter

Overview

Introduction

The Remote Office 9150 unit provides full-featured host Meridian 1 PBX services to as many as 32 users located in your office.

Components

The Remote Office 9150 solution consists of the following components:

- Meridian Internet Gateway Reach Line Card (MIG RLC)

  The MIG RLC is installed in the Meridian 1 PBX at the host location and relays voice and signaling information from the digital telephones connected at the Remote Office 9150 site to the Meridian 1 PBX at the host site.

- Remote Office 9150 unit

  The Remote Office 9150 unit is installed in your office. It relays voice and signaling information between the digital telephones in your office to the Meridian 1 PBX at the host location.

- 10BaseT Ethernet and ISDN Basic Rate Interface (BRI) connections

  These connections provide the voice and data connections between the Remote Office 9150 unit and the host PBX.

- ISDN BRI trunk interface modules are supported for the following:
  - U interface
  - S/T interface
- optional Digital Signal Processor (DSP) application modules

  You can add these modules to increase the system’s voice processing capacity.

What does the Remote Office 9150 unit do?

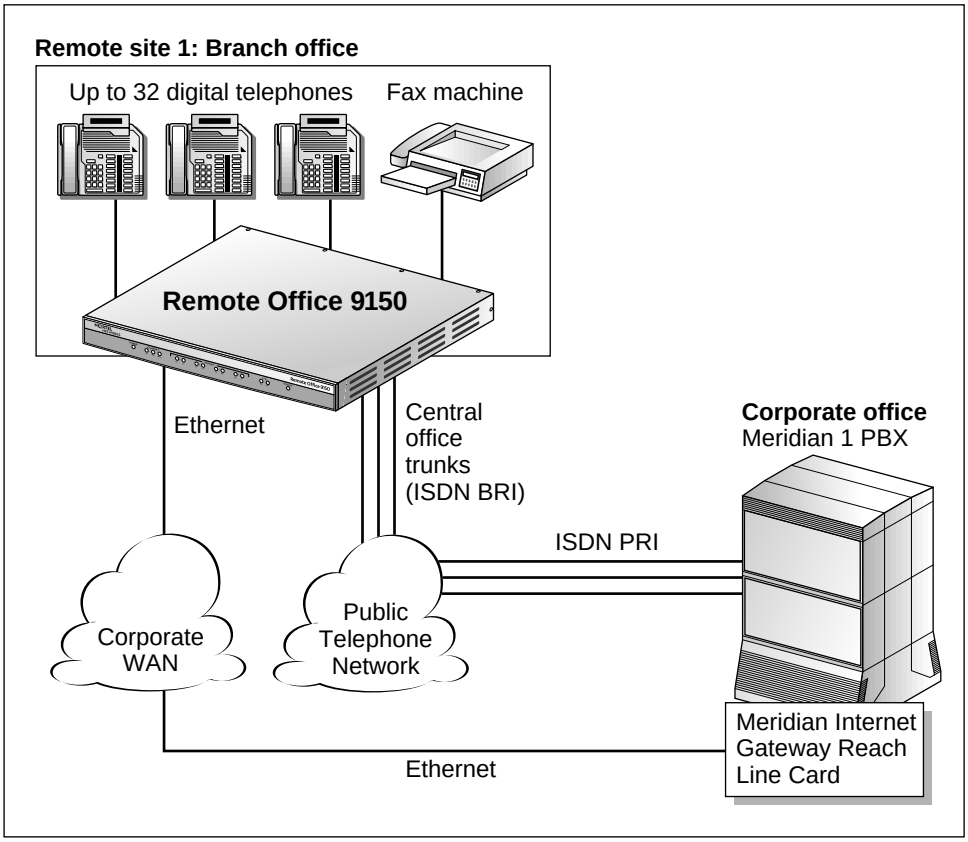
The Remote Office 9150 unit uses the Voice over IP technology to route voice conversation and phoneset control signals between your office and the host PBX over your existing IP data network. The Remote Office 9150 unit can also route calls over the circuit-switched network.

This is accomplished using the following components:

- the Remote Office 9150 unit located in your office
- the MIG RLC located on the Meridian 1 PBX at the host site

These two components, along with the 10BaseT Ethernet and ISDN BRI connections, extend the host PBX services to users in your office.

The illustration below shows the connection between a Remote Office 9150 unit and a MIG RLC.



Telephone call modes

Calls can be placed through the Remote Office 9150 unit in any of the following modes:

- host-controlled mode

  When a call is processed through the host PBX, the call is in host-controlled call mode. The call can be routed over the IP network or the circuit-switched network.

- local-controlled call mode

  When a call is processed through the local PSTN, the call is in local-controlled call mode.

Placing calls

To place a call in host-controlled mode, users can pick up the handset or press the primary (host) line key, and then dial the number of the party they are calling.

To place a call in local-controlled mode, users can pick up the handset or press the secondary (local) line key, and then do one of the following:

- to place an external call: dial the trunk access code to obtain an outgoing trunk, then dial the number of the party they are calling
- to place an internal call: dial the extension of another station in the same office

Product features

The Remote Office 9150 unit offers the following features:

- system security that supports three security levels—no security, calling line identification (CLID), and security identifier
- trunking allocation that automatically allocates trunk bandwidth as it is needed
- support for Meridian digital telephones, telephone modules, and standard calling features
- Voice over IP features that automatically switch from the IP network to the circuit-switched network when the voice Quality of Service (QoS) falls below a predetermined threshold, and back to the IP network when the QoS returns to normal

  Voice packet features include voice compression, jitter attenuation, and silence suppression.
- permanent or demand connections

  If the connection is defined as call on demand, minimum call duration and idle timers can be configured.

- single ports, multi-user ports, and dynamic port pooling that assigns users to the first available port
- the ability to ensure QoS for specific users

  This is done by assigning more priority to those users. There are four levels of priority:

  - high
  - normal
  - IP only
  - circuit-switched only
- local calling that allows you to place calls to other extensions within your office, or to telephones in your local community
- an online/offline table that is configured on the MIG RLC for scheduling times
  - that the ISDN BRI connection to the host PBX is made available to the Remote Office 9150 site

    Note: When the Remote Office 9150 unit is in offline mode, calls cannot be made or received through the host PBX over the IP or circuit-switched network.
  - at which all telephones in your office can use only the local PSTN service

  This allows you to ensure that unwanted ISDN BRI telephone calls through the host PBX are disabled after business hours.
- an emergency service number that can be programmed with your local emergency number
- an analog port that can send and receive faxes
- administrative tools that allow you to perform a variety of administrative tasks, such as
  - changing the administration password
  - making configuration changes
  - viewing the system logs and statistics
  - performing upgrades, backups, and restores

Section A: Product description

In this section

Overview

Introduction

This section provides a brief description of each Remote Office 9150 unit feature.

Hardware

The Remote Office 9150 unit is installed in your office and can be mounted on a desk, in a rack, or on the wall. The unit contains LED displays and network connectors, and is shipped with a 110/220 V power supply and an RS-232 serial cable.

Add-on modules

The Remote Office 9150 unit can support up to four ISDN BRI (U or S/T) trunk interface modules and up to three Digital Signal Processor (DSP) application modules.

Connection options

Communications between the Remote Office 9150 unit in your office and the MIG RLC on the host PBX take place using 10BaseT Ethernet and ISDN Basic Rate Interface (BRI) connections. An analog port for fax machines is also provided.

How the Remote Office 9150 unit works

There are two major components to the Remote Office 9150 unit:

- the Remote Office 9150 unit located in your office
- the MIG RLC located on the Meridian 1 PBX at the host site

These two components, along with the connection options described on page 19, extend the host PBX services to users in your office.

The Remote Office 9150 unit can operate in

- host-controlled mode: calls are routed through the host PBX
- local-controlled mode: calls are routed through the local PSTN, or to other stations in the same office

To understand how calls are routed in the various modes, see the sample illustrations beginning on page 24.

What is Remote Office 9150?

Introduction

Remote Office 9150 is a product that provides full-featured host Meridian 1 PBX services to as many as 32 users located in your office.

The Remote Office 9150 unit uses the Voice over IP technology to route voice conversation and phoneset control signals between your office and the host PBX over your existing IP data network.

The Remote Office 9150 unit can also use the circuit-switched network to route calls if

- the voice QoS degrades below predefined thresholds

  In this case, Nortel Networks' patented QoS transitioning technology automatically transitions calls to the circuit-switched network when the voice QoS degrades. Calls transition back to the IP network when the QoS returns to normal.

- you are not yet ready to use the IP network to route voice calls

  You can configure the Remote Office 9150 unit to use only the circuit-switched network, and implement the IP network functionality when you are ready.

This section provides a brief description of each component used in a Remote Office 9150 system.

Meridian Internet Gateway Reach Line Card

The Meridian Internet Gateway Reach Line Card (MIG RLC) is installed in the Meridian 1 PBX at the host location. The MIG RLC provides service for up to 16 ports on a 1-slot card, or 32 ports on a 2-slot card. It emulates a standard digital line card (XDLC), providing PBX functionality for telephones at remote locations (including sites using the Remote Office 9150 unit).

The MIG RLC relays voice and signaling information between the digital telephones connected at the Remote Office 9150 site to the Meridian 1 PBX at the host site. Like the Remote Office 9150 unit, the MIG RLC can route calls over the IP network or the circuit-switched network, or both when the QoS transitioning technology feature is configured.

For a more detailed description, refer to the *Meridian Internet Gateway Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

Remote Office 9150 unit

The Remote Office 9150 unit installed in your office provides PBX functionality for up to 32 digital telephones. Voice and signaling information between the digital telephones connected at your office and the MIG RLC installed on the Meridian 1 PBX at the host location is relayed over one or both of the following:

- IP network
- circuit-switched network

For more details, see “Remote Office 9150 hardware description” on page 13.

10BaseT Ethernet and ISDN BRI connections

These connections provide the voice and data connections between the Remote Office 9150 unit and the host PBX. See “Connection options” on page 19 for a more detailed description.

Optional trunk interface modules

You can install up to four ISDN BRI U or S/T interface modules in the Remote Office 9150 unit. They provide the interface to the ISDN BRI lines provided by your telephone service provider, and are used to route calls over the circuit-switched network.

Optional Digital Signal Processor application modules

You can install up to three Digital Signal Processor (DSP) application modules to increase the Remote Office 9150 unit’s voice processing capacity. (See “Add-on modules description” on page 17).

Configuration Manager

Use the following tools to configure the Remote Office 9150 unit:

- for first-time configuration: Configuration Wizard

  The Configuration Wizard provides the ability to configure only the minimum information needed to get the Remote Office 9150 unit up and running.

  For more details, see “Using the Configuration Wizard to perform initial configuration” on page 141.

- for ongoing configuration and administration: Configuration Manager

  For more details, see the following:

  - Chapter 4, “Configuration Manager overview”
  - Chapter 5, “Configuring the Remote Office 9150 unit”
  - Chapter 7, “Administration”

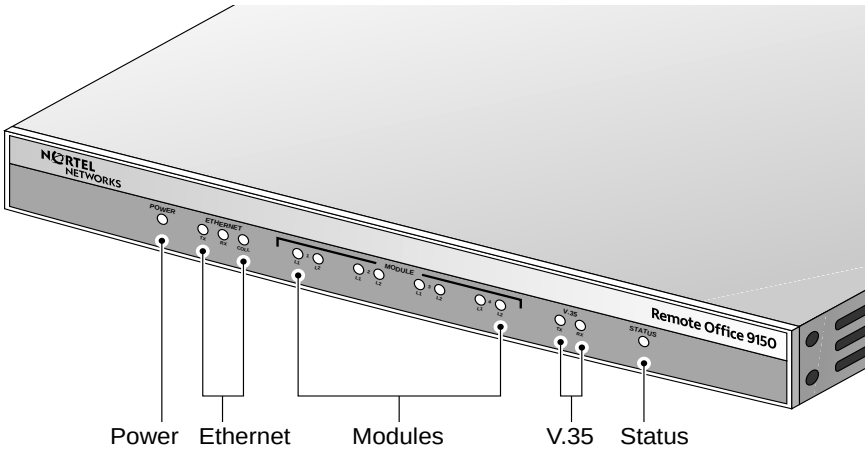
Remote Office 9150 hardware description

Introduction

The Remote Office 9150 unit is installed in your office and can be mounted on a desk, in a rack, or on the wall. This section describes the LED displays, power supply, cables, and connectors for the unit.

LEDs on the Remote Office 9150 unit

The following diagram shows the LEDs on the front panel of the Remote Office 9150 unit.



Note: The V.35 LEDs are for future use.

G101402

The operational status of the Remote Office 9150 unit is indicated by these LEDs as described in the following table.

LED type	LED name	Description
Power	On	When lit, this LED indicates that power is present.
Ethernet	COLL	When flashing, this LED indicates that a collision has occurred on the Ethernet network.
	TX	When flashing, this LED indicates that data is being transmitted by the Remote Office 9150 unit over the Ethernet network.
	RX	When flashing, this LED indicates that data is being presented to the Remote Office 9150 unit over the Ethernet network.
Module	L1 and L2	L1 LED: ■ not lit: there is no D-channel activity ■ flashing: the D-channel is active but the B-channel is not active ■ lit solid: both the D- and B-channels are active L2 LED: ■ not lit: the B-channel is not active ■ lit: the B-channel is active
V.35	TX	For future use.
	RX	For future use.
Boot status	Status	Indicates the health of the Remote Office 9150 unit. This LED stays lit when the power on self-test is successful. If it goes out, there is a problem.

Note: Since Ethernet traffic has a nominal speed of 10 Mbps, the flashing Ethernet COLL, TX, RX LEDs are cosmetic. They do not reflect real-time traffic patterns or packets.

Connectors

The following connections are made from the rear panel of the Remote Office 9150 unit to the telephone and data networks:

- Two 25-pair connectors (labeled TELCO 1 and TELCO 2) provide tip and ring connections to user stations (telephones) and central office trunks (ISDN BRI).

  These connections provide the interface to the telephone network and the Public Switched Telephone Network (PSTN).

- An RJ-45 connector (labeled ETHERNET) provides a 10BaseT Ethernet connection.

  This connection provides the ability to pass both voice and data traffic over the existing Ethernet network.

- A DB-9 connector (labeled ADMIN) provides an RS-232 serial port connection.

  You can use this serial port connection to configure a Remote Office 9150 unit that is directly connected to a PC.

- The DB-25 connector (labeled V.35) is for future use.

Refer to Chapter 2, “Planning for installation,” for a detailed description of cables and connectors.

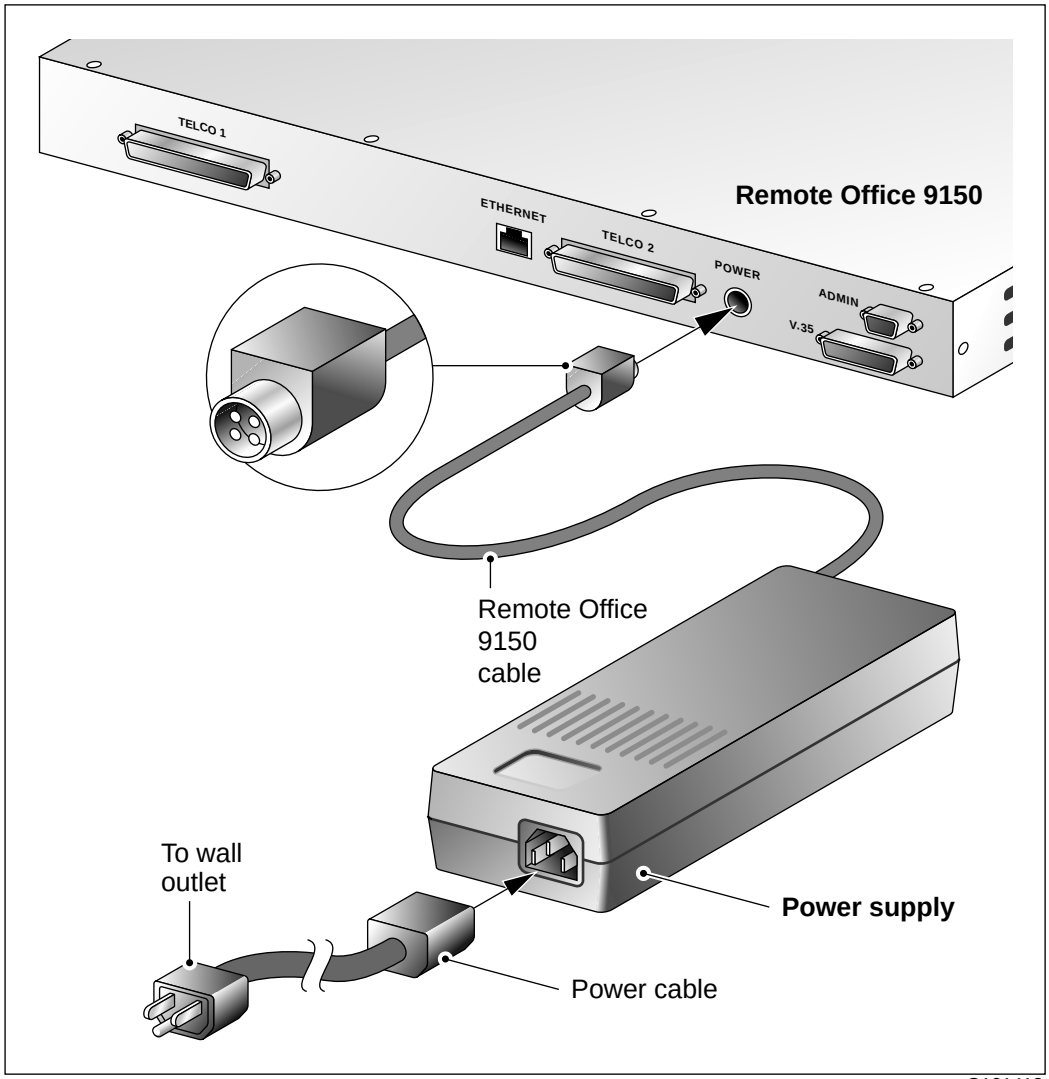
Mounting options

The Remote Office 9150 unit can be mounted on a desk, in a rack, or on the wall.

Universal power supply

The Remote Office 9150 unit includes an auto-sensing 110/220 V power supply that is compatible with commercially available UPS systems. See the diagram on page 16.

Remote Office 9150 power supply



G101412

Add-on modules description

Introduction

The Remote Office 9150 unit can support trunk interface modules, such as ISDN BRI U or S/T interfaces, and up to three DSP application modules.

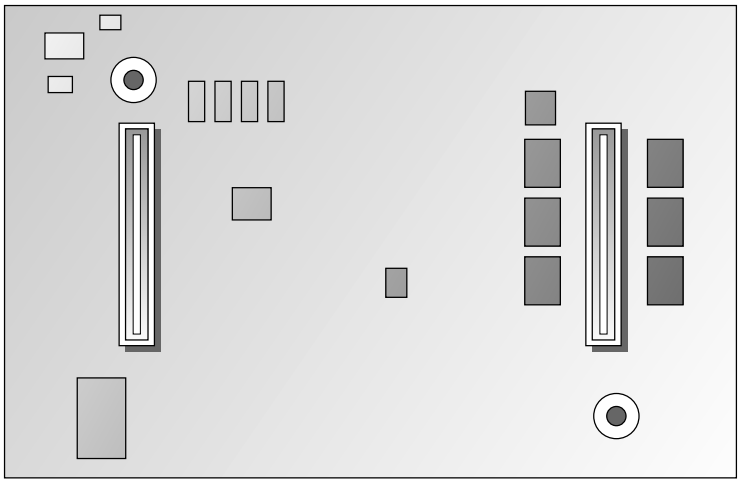
Optional trunk interface modules

The Remote Office 9150 unit can support up to four U or S/T ISDN BRI interfaces. Each module supports one ISDN BRI line (with two B-channels) from the local telephone service provider.

Initially, the Remote Office 9150 unit ships with no ISDN BRI modules installed.

ISDN BRI module

Remote Office ISDN BRI module



U interface (NTDR74xx)
S/T interface (NTDR75xx)

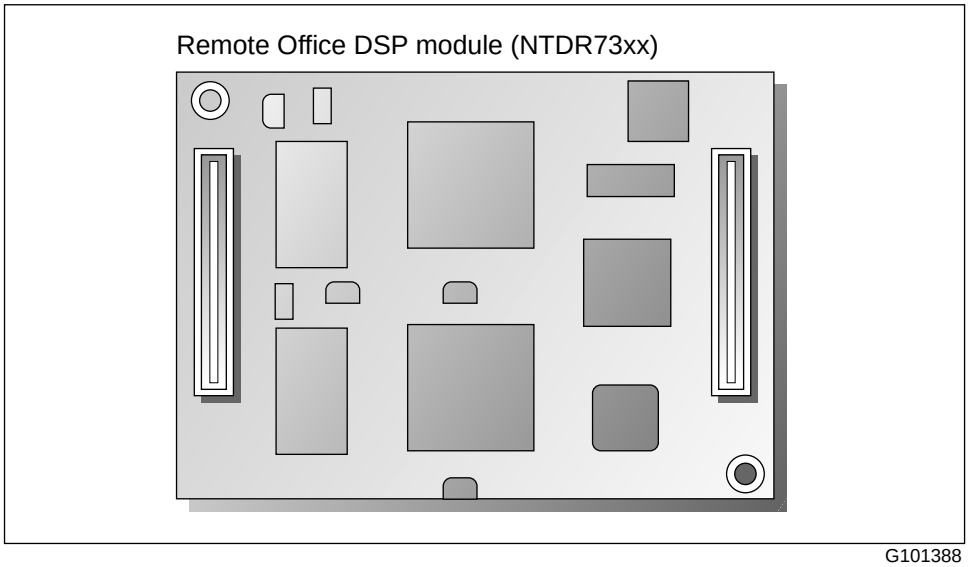
G101420

Optional DSP application modules

DSPs convert voice and fax into digital data for transport over the IP and circuit-switched networks. Initially, the Remote Office 9150 unit ships with the ability to support up to eight simultaneous calls through a DSP that is built into the Remote Office 9150 unit's motherboard. To add support for up to 32 simultaneous calls, you must install DSP application modules. Up to three DSP application modules are supported. Each module provides up to eight more simultaneous calls.

In addition, you can configure the Remote Office 9150 unit for blocking with only enough modules to support the maximum number of simultaneous calls. For example, a Remote Office 9150 unit that is equipped with a single DSP application module supports 16 simultaneous calls, for a ratio of 2:1 blocking. For more details, see "Planning for future growth" on page 94.

DSP application module



Connection options

Introduction

Communications between the Remote Office 9150 unit in your office and the host PBX take place using 10BaseT Ethernet or ISDN BRI connections, or both. This section provides a description of each of these connections.

10BaseT Ethernet interface

Voice over IP technology is used to carry voice conversation and phoneset control signals over your IP network to the host PBX. The voice data is forwarded as UDP/IP packets, and the signaling data is forwarded as TCP/IP packets.

ISDN BRI lines to PSTN

The PSTN provides a cost-effective alternative to leased lines. You can use ISDN BRI lines at the Remote Office 9150 site to make local calls without involving the host PBX. You can also choose to use the ISDN BRI lines instead of the IP network to route calls through the host PBX.

To use ISDN BRI lines, you must install trunk interface modules. The Remote Office 9150 unit can support up to four U or S/T ISDN BRI trunk interface modules. (See “Add-on modules description” on page 17.)

Quality of Service transitioning technology

If both the IP network and ISDN BRI lines are used, you can use the QoS transitioning technology to reroute calls from the IP network to the circuit-switched network when the QoS on the IP network degrades. When the QoS returns to normal, the QoS transitioning technology automatically moves the calls back to the IP network.

The Remote Office 9150 unit monitors the QoS on the IP network. If the QoS falls below preprogrammed acceptable thresholds, calls are dynamically and transparently switched to the ISDN BRI lines. See “Quality of Service transitioning technology” on page 45 for additional details.

Analog port for fax machines

The Remote Office 9150 unit has one analog port that you can use as a fax connection. See “Fax support” on page 59 for more detailed information.

How the Remote Office 9150 unit works

Introduction

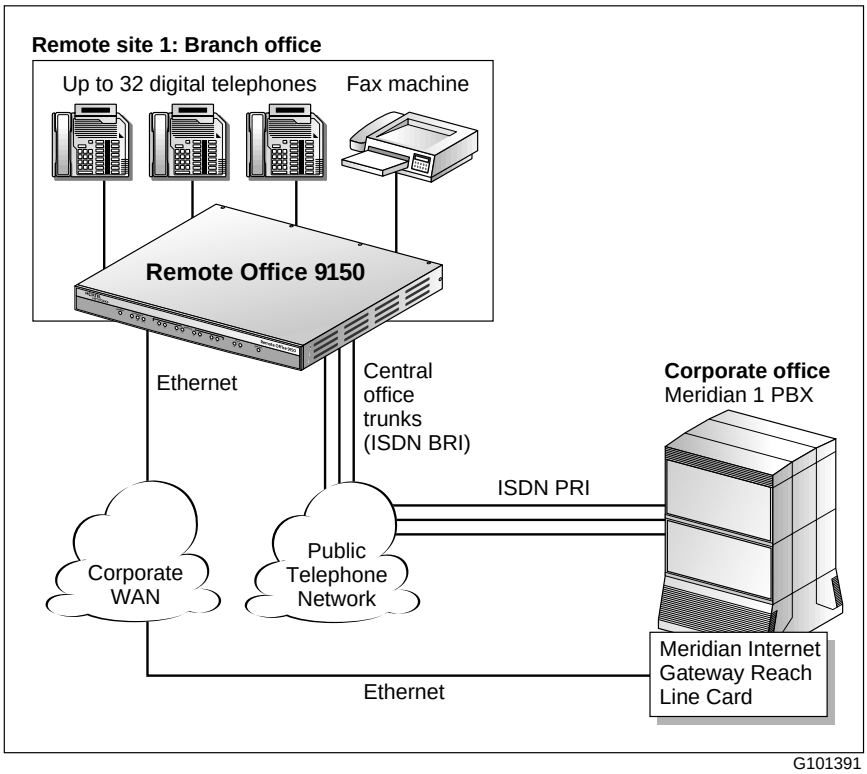
There are two major components to the Remote Office 9150 product:

- the Remote Office 9150 unit located in your office
- the MIG RLC located on the Meridian 1 PBX at the host site

These two components, along with the connection options described on page 19, extend the host PBX services to users in your office.

Network diagram

The following diagram shows a MIG RLC and Remote Office 9150 network.



Outgoing call process

To place outgoing calls, users can either pick up the handset on the telephone or press a line appearance key. There are two types of line appearance keys:

- host call appearance key

  Use this key to make a call through the host PBX.

- local call appearance keys

  Use these keys to make calls to other stations in your office, or to make and receive calls through the local PSTN. You can define up to two local call appearance keys on each digital telephone.

For a detailed description of the outgoing call process, see the sample illustrations beginning on page 24.

Incoming call process

When a user places a call through the host PBX to a user at the Remote Office 9150 site, a connection is made from the MIG RLC to the Remote Office 9150 unit and the host PBX completes the call normally. If a connection cannot be established, then the call rings until it is forwarded to voice mail by the host PBX. See Chapter 6, “Using Remote Office 9150 stations,” for a more detailed description of the incoming call process.

When someone places a call through the PSTN to a user at the Remote Office 9150 site, a connection is made from the central office to the Remote Office 9150 unit. The number that outside callers dial is the number assigned by the ISDN service provider to the ISDN BRI B-channel on which the incoming call is received.

If the incoming local call is not answered, the call is forwarded to one of the following:

- to the same voice mail provided by the host PBX

  To accomplish this, the station must be configured with both local and remote calling capability. The host PBX voice mail service is not available for stations that are defined as local only.

- to another extension in the same office

  To accomplish this, one of the local feature keys on the phoneset must be defined as Call Forward with the DN of the station to which calls should be forwarded.

Host controlled call mode

When a user places a call to someone at the host site, or when someone from the host site calls the Remote Office 9150 site, the call is in host-controlled call mode. Calls in host-controlled mode are routed through the host PBX. See the sample illustrations on pages 24 and 26.

Local-controlled call mode

When a user places a call from a local call appearance key, or the call is to another telephone at the Remote Office 9150 site, the call is in local-controlled mode. Calls that are initiated from the local call appearance key are routed through the local PSTN. Calls to other extensions in the Remote Office 9150 site are routed only through the Remote Office 9150 unit.

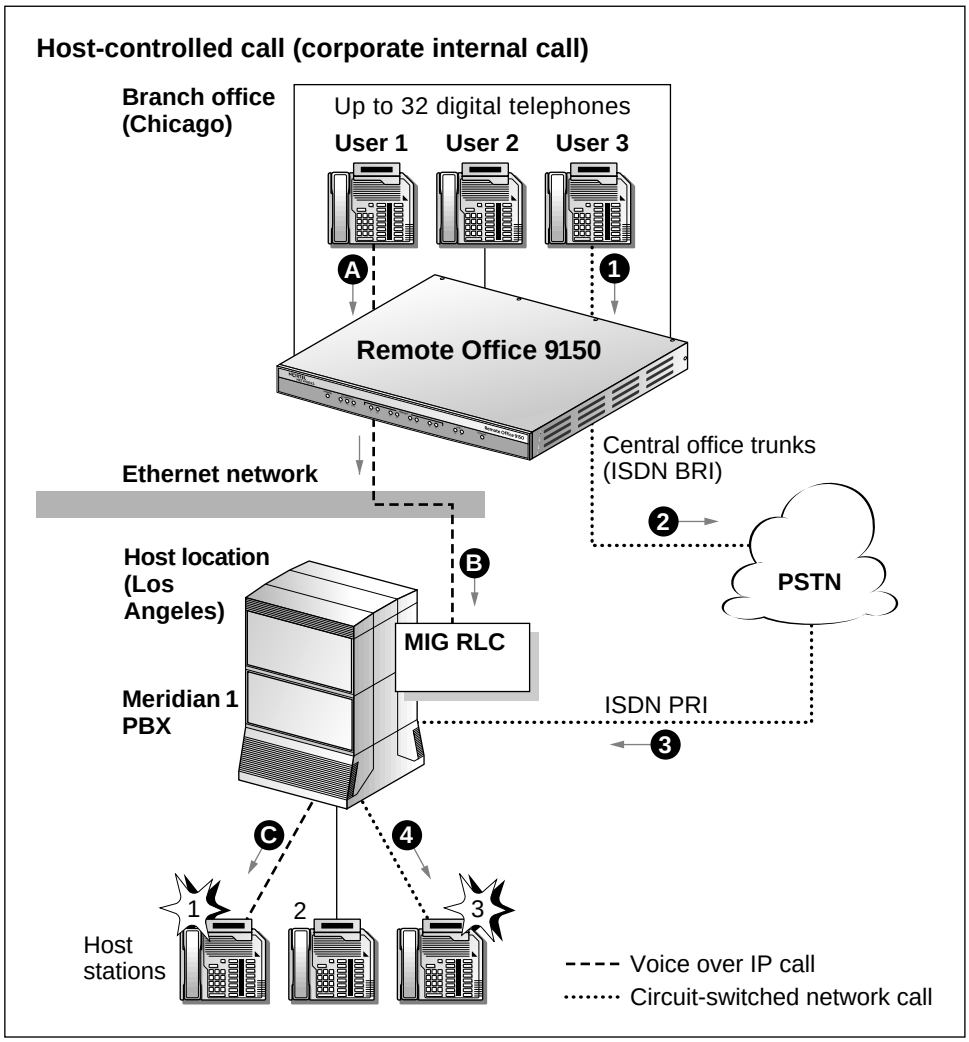
The host PBX is not involved in local-controlled mode calls. See the sample illustration on page 28.

Quality of Service transitioning technology

If the QoS on the IP network falls below a predefined threshold, you can configure the Remote Office 9150 unit to automatically route voice traffic away from the IP network connection to the circuit-switched connection. See “Quality of Service transitioning technology” on page 45 for a detailed description.

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.



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.

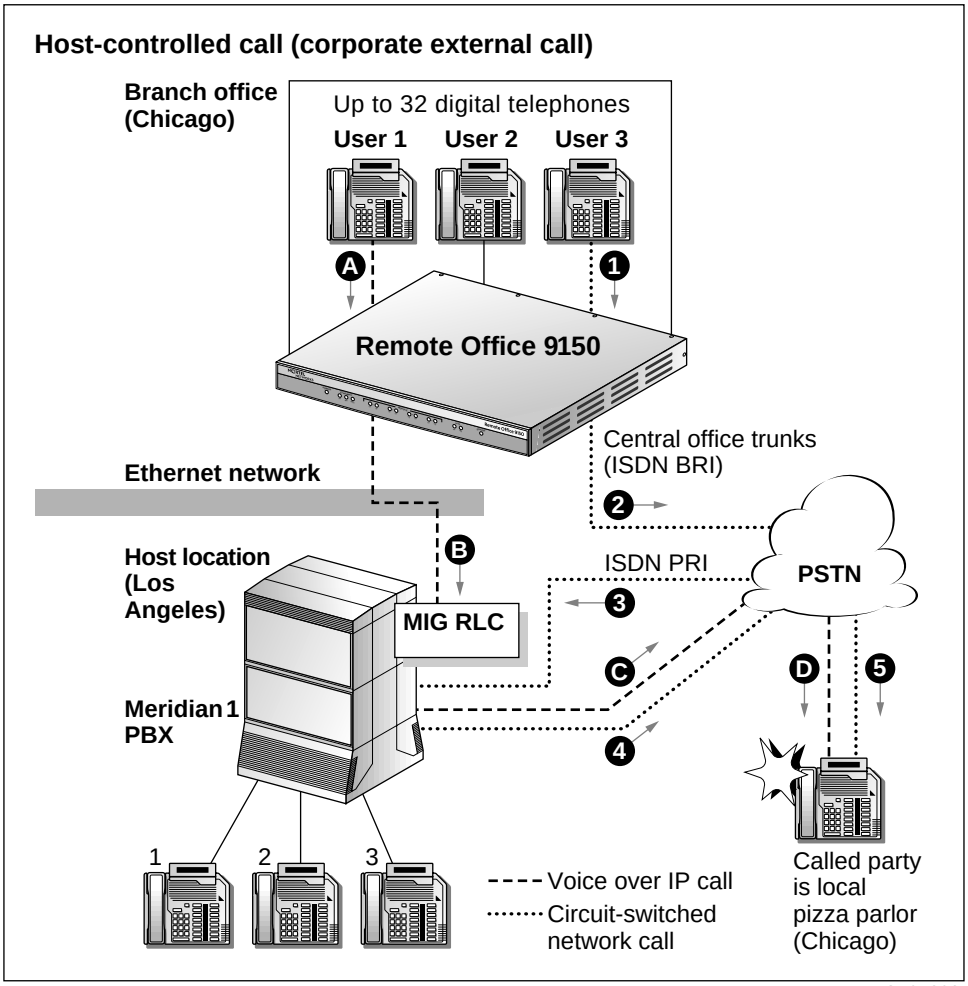
Result: User 3 hears a dial tone. This indicates that the connection to the MIG RLC over the circuit-switched network was successful.

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.



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.

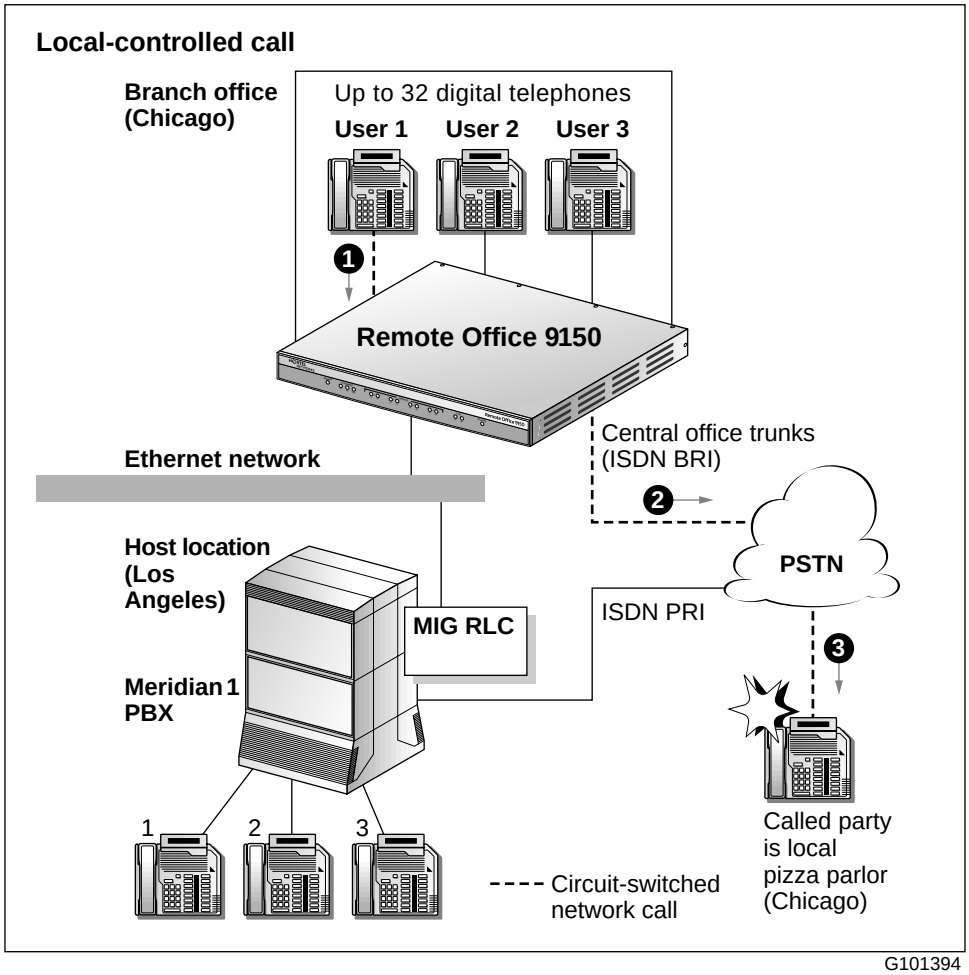
Result: User 3 hears a dial tone. This indicates that the connection to the MIG RLC over the circuit-switched network was successful.

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 your local area.



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 #61) 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.

Section B: Feature description

In this section

Overview

Introduction

This section provides a brief description of each Remote Office 9150 feature.

System security

The Remote Office 9150 unit supports three security levels—no security, calling line identification (CLID), and security identifier. The security levels control access from the Remote Office 9150 unit to the MIG RLC on the host PBX.

Trunking

The Remote Office 9150 unit automatically allocates trunk bandwidth as it is needed. For example, as calls are initiated and bandwidth requirements increase, additional trunk connections are established. Likewise, as calls terminate and bandwidth requirements drop, idle trunks are shut down.

Telephones

The Remote Office 9150 unit supports Meridian digital telephone, telephone modules, and standard calling features.

Voice over IP features

You can configure the MIG RLC port to which the Remote Office 9150 unit is assigned to automatically move calls from the IP network to the circuit-switched network when the voice QoS falls below a predetermined threshold. When QoS returns to normal, calls are moved back to the IP network.

Call on demand versus permanent connections

The ISDN connection between the MIG RLC and Remote Office 9150 unit can be a permanent or call on demand connection. The connection type is defined on the MIG RLC port to which the Remote Office 9150 unit is assigned.

A permanent connection means the ISDN connection to the host PBX always remains open. A call on demand connection means the ISDN connection opens only when a connection with the host PBX is required.

If the connection is defined as call on demand, minimum call duration and idle timers can be configured on the MIG RLC. This helps to reduce ISDN BRI charges.

Port management

Each port on the MIG RLC can be defined as one of the following port types:

- single-user port

  Each single-user port supports one remote station at the Remote Office 9150 site.

- multi-user voice port

  Up to eight persons can share the same MIG RLC port, but not at the same time. This port type is especially useful for employees who are working in mutually exclusive shifts. All stations that use this type of port respond to the same DN and have identical phoneset configurations.

- a port in a dynamic port pool

  This is similar to a multi-user port except that the persons who share ports in a dynamic pool are assigned to the next available port in the MIG RLC port pool. There is no correlation between the station and the port on the MIG RLC.

  This feature is especially useful in free-seated ACD environments where agents log on to the host PBX using their agent IDs.

The MIG RLC administrator can tell you which port types are used by your office.

Station priority

One of the following priority levels can be assigned to each station:

- high
- normal
- circuit only
- IP only

The priority level is defined on the MIG RLC port to which the station is assigned. For more details, see “Station priority” on page 52.

Local calling

The Remote Office 9150 unit allows you to place calls to other extensions within your office, or to telephones in your local community. This is accomplished through the use of up to two local call appearance keys.

Note: If a user initiates the call from the host call appearance key, the station-to-station call requires transmission of signaling data through the host PBX.

Online/offline table

The online/offline table is configured on the MIG RLC and allows you to schedule times

- when the Remote Office 9150 unit’s ISDN BRI connection to the host PBX can be active

  Note: When the Remote Office 9150 unit is in offline mode, users cannot make or receive calls through the host PBX over the IP or circuit-switched network.
- when all telephones in your office can use only the local PSTN service

This allows you to ensure that costly ISDN BRI telephone calls through the host PBX are disabled after business hours.

Fax support

The Remote Office 9150 unit contains a full-featured analog port that can send and receive faxes.

Emergency service number

If you are using the circuit-switched network to route calls, you can program an emergency service number (such as 911) on the Remote Office 9150 unit. This allows the emergency service call to be routed through the local PSTN instead of through the host PBX, regardless of which call appearance key (host or local) was used to initiate the call.

Note: If you are using only the IP network to route calls, you should make emergency service calls on a telephone that is directly connected to a PSTN line. If you make an emergency service call from a station that is connected to the Remote Office 9150 unit, the call is routed through the host PBX, which could be in a different city.

Administrative tools

The Configuration Wizard and Configuration Manager software allow you to perform configuration. Configuration Manager also allows you to perform a variety of administration tasks on the Remote Office 9150 unit, such as

- changing the administration password
- viewing the system logs and statistics
- performing upgrades, backups, and restores

System security

Introduction

This section describes the security levels that are supported for controlling access from the Remote Office 9150 unit to the MIG RLC on the host PBX.

No security

When no security measures are used, the MIG RLC accepts all incoming calls from the Remote Office 9150 site.

Use this level with caution as it can be prone to unauthorized use. For example, a user in your site could accidentally, or intentionally, enter a trunk number for another site and place long distance phone calls through this connection.

Calling Line Identification

When Calling Line Identification (CLID) is used, and the circuit-switched network is used to route the call, the MIG RLC identifies the Remote Office 9150 unit's CLID. If the CLID matches the remote number configured on the port assigned to the Remote Office 9150 unit, access is granted. If the incoming call's CLID does not match, access is denied.

Caller ID authentication cannot be performed over the IP network.

Security identifier

You can use security identifier authentication over the IP or circuit-switched network. When security identifier is used, the Remote Office 9150 unit sends its security identifier (password) for each connection request. The MIG RLC compares the identifier configured on the MIG RLC port to which the Remote Office 9150 unit is assigned. If the identifiers match, access is granted.

If the identifiers do not match, an event is recorded in the Remote Office 9150 unit system log, which can be viewed in Configuration Manager. The telephone that was used to make the call displays a message indicating that communications with the host PBX are down.

Trunking, connection types, and call timers

Introduction

This section describes what is supported on the circuit-switched network.

Trunk connections

The following digital trunk connections are supported:

- ISDN BRI from the Remote Office 9150 unit to the PSTN
- ISDN PRI from the PSTN to the MIG RLC at the host site

Bandwidth allocation

The MIG RLC automatically allocates trunk bandwidth to the Remote Office 9150 connection as it is needed. For example, as calls are initiated and bandwidth requirements increase, additional trunk connections are established. Likewise, as calls terminate and bandwidth requirements drop, idle trunks are shut down.

Connection types

The Remote Office 9150 connection to the MIG RLC can be defined on the MIG RLC as a permanent or demand connection. A permanent connection means that the ISDN connection to the host PBX always remains open. A demand connection means that the ISDN connection opens only when a connection with the host PBX is required.

If the connection is defined as demand, then you can configure minimum call duration and idle timers on the MIG RLC to help reduce call charges.

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: 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 has 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.

Telephones

Introduction

This section lists the telephones, features, and modules supported by the Remote Office 9150 unit.

Supported digital telephones

The following Meridian digital telephones are supported:

M2008D	M2616CT	M3902
M2008HFD	M3110	M3903
M2216D	M3310	M3904
M2616D	M3820	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.

Supported telephone modules

The following telephone modules are supported:

- add-on modules (to add more keys)
- application modules that provide more functionality
- Meridian Communication Adapters (MCA)
- Analog Telephone Adapters (ATA)

Supported telephone features

All features provided by the host PBX are supported for host-controlled calls. The following are some examples:

- Hold
- Call Waiting
- Transfer
- Conference
- Call Forward
- ACD features
- Paging

See Chapter 6, “Using Remote Office 9150 stations,” for a detailed description of the above features.

Computer telephony integration applications

There are two types of computer telephony integration (CTI) applications:

- first-party CTI applications that use the Symposium Desktop TAPI Service Provider
- third-party CTI applications that use Symposium TAPI Service Provider for M1

Both types can be used with the Remote Office 9150 unit.

TAPI Type	Supported CTI Application
Symposium Desktop TAPI Service Provider 1.6	■ Symposium FastView 1.6 ■ Symposium FastCall 1.6 ■ Symposium Call Manager 5.0 ■ other TAPI-compliant applications
Symposium TAPI Server Provider for Meridian 1 Release 2.1	■ Symposium Agent 1.1 ■ Symposium Call Manager 5.0 ■ other Symposium Partner products

You can use first-party CTI applications with the Remote Office 9150 unit if

- your PC is equipped with a Symposium Communicator card version 1.2 with software version 2.0
- your digital telephone is equipped with a Meridian Communications Adaptor (MCA)

Note: The Symposium Communicator Card is not available in all countries. Check with your Nortel Networks distributor for availability.

Automatic Call Distribution (ACD) applications

The Remote Office 9150 unit supports all Nortel Networks ACD applications.

Voice over IP features

Introduction

You can configure the Remote Office 9150 unit to use the following Voice over IP features:

- Convert analog voice into digital data for transmission as voice packets over the network for calls to or from the fax machine or other analog device that is connected to the analog port on Telco 1.
- Automatically switch from the IP network to the circuit-switched network when the voice QoS falls below a predetermined threshold, and back to the IP network when the QoS returns to normal.

Packetized voice

DSPs located in the Remote Office 9150 unit convert voice into digital data packets and, if compression is used, compresses them. The data is constructed as UDP/IP voice packets for transmission over the IP network.

When voice packets are compressed, they consume less bandwidth, leaving more bandwidth for data or other voice or fax communications. The following algorithms are supported:

- G.711: Packets are transmitted at 64 Kbps (that is, they are not compressed).
- G.726: Packets are compressed and transmitted at 32 Kbps.
- G.729A: Packets are compressed and transmitted at 8 Kbps.

G.729A is the default algorithm on both the MIG RLC and the Remote Office 9150 unit.

In addition to voice compression, the Remote Office 9150 unit supports the following additional packetized voice features:

- A voice jitter attenuation buffer removes the variable delays from the voice packets sent across the IP network, thus avoiding awkward-sounding speech.

- Packet loss handling techniques accommodate missing packets or packets received too late to be processed.
- Silence suppression prevents packet transmission during periods when there is no voice data present. Comfort noise is inserted to assure the user that the line is still active.

  Silence is determined when the difference between the adaptable noise floor and the detected signal is less than 9 dB. To prevent clipping, silence must be present for a minimum of 250 milliseconds.

Quality of Service transitioning technology

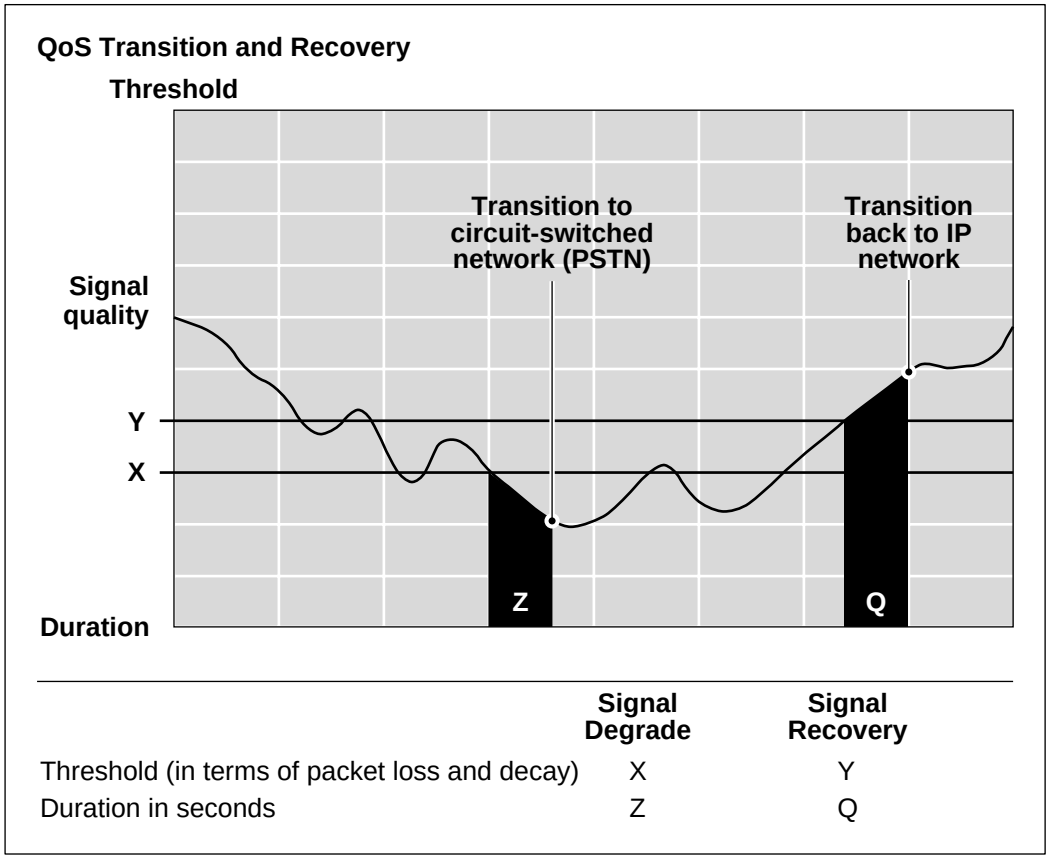
Communications between the Remote Office 9150 unit in your office and the host PBX take place across the IP network using a 10BaseT Ethernet interface. You can configure the Remote Office 9150 unit to switch automatically from the IP network to the circuit-switched network when the voice QoS falls below a predetermined threshold.

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

For detailed instructions on configuring the thresholds, refer to the *Meridian Internet Gateway Reach Line Card Installation and Administration Guide* (NTP 555-8421-210). 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 illustration on the next page shows how the QoS transitioning technology works.



The following table describe the threshold and duration settings shown in the diagram. These settings are configured on the MIG RLC port to which the Remote Office 9150 unit is assigned.

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.

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.
Z	Represents the amount of time that signal quality must be lower than the X threshold before calls transition to the circuit-switched network.
Q	Represents the amount of time that signal quality must be higher than the Y threshold before calls transition 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 Remote Office 9150 unit establishes a PSTN network connection to the MIG RLC on the host PBX.

   The Remote Office 9150 unit 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. An IP test is run to determine if the QoS has been restored on the IP network. See “Offline IP network measurements” on page 49.
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 Remote Office 9150 unit monitors the following QoS parameters:

- average packet delay

  The delay is calculated using the following statistics gathered from the Remote Office 9150 unit’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 Remote Office 9150 unit 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 Remote Office 9150 unit 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 Office 9150 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 324).

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

Port management

Introduction

You can assign Remote Office 9150 stations to one of the following types of MIG RLC ports:

- single-user ports
- multi-user voice ports
- dynamic port pool

Port types are assigned on the MIG RLC. Refer to the *Meridian Internet Gateway Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) for detailed instructions.

Single-user ports

Each port that is defined as a single-user (dedicated) port on the MIG RLC supports one Remote Office 9150 station.

Multi-user ports

Ports that are defined on the MIG RLC as multi-user ports allow multiple stations on different Remote Office 9150 units to time-share a single port on the host PBX.

Up to eight persons can share the same MIG RLC port, but not at the same time. All stations that use this type of port must respond to the same DN and have identical phoneset configurations. This port type is especially useful for employees who are working in mutually exclusive shifts.

Dynamic port pool

Dynamic port pooling is similar to a multi-user port except that the persons who share ports in a dynamic pool are assigned to the next available port in the MIG RLC port pool. There is no correlation between the station and the port on the MIG RLC.

This feature is especially useful in free-seated ACD environments where agents log on to the host PBX using their agent IDs.

Station priority

Introduction

You can define a MIG RLC port to which a station is assigned as normal priority, high priority, circuit-switched only, or IP only.

Normal priority

When both the IP and circuit-switched networks are used to route calls, calls to and from the station are routed primarily over the IP network (if the IP network is used to route calls). Calls transition between the IP and circuit-switched networks whenever voice QoS levels change. (The voice QoS levels are defined on the Quality of Service screen on the MIG RLC for your Remote Office 9150 unit.)

High priority

When both the IP and circuit-switched networks are used to route calls, calls to and from the station are routed primarily over the IP network. Calls transition between the IP and circuit-switched networks whenever voice QoS levels change. (The voice QoS levels are defined on the Quality of Service screen on the MIG RLC for your Remote Office 9150 unit.)

When the priority reservation setting is also defined on the connection between the MIG RLC and the Remote Office 9150 unit, the following benefits are provided:

- If allowed to use the IP network to process calls (this is transparent to the user), an active call on that station is always one of the first to be transitioned to PSTN trunks when Voice over IP QoS has degraded. (This transition is accomplished using the QoS transitioning technology.)
- Call blocking is reduced because bandwidth is always available to these stations.

  Note: If the reserved bandwidth is being used by other high priority stations, then new calls are processed using unreserved bandwidth.

The number of stations that can be configured as high priority depends on the amount of available bandwidth. Ensure that enough bandwidth is available to process calls on normal priority stations.

IP only

Calls to and from the station are routed over the IP network only (if the IP network is used to route calls). QoS transition is not available for stations that are defined as IP only.

Circuit only

Calls to and from the station are routed over the circuit-switched network only (if the circuit-switched network is used to route calls). Circuit only stations never experience voice QoS degradation.

Connection bandwidth

Introduction

On the connection between the MIG RLC and the Remote Office 9150 unit, you can configure the following:

- when to open additional B-channels (referred to as *extra bandwidth*)
- how much bandwidth to reserve for high priority stations (referred to as *priority reserved bandwidth*)

For instructions, refer to “Configuring ports” in the *Meridian Internet Gateway Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

Extra bandwidth

When available bandwidth is no longer sufficient to process active calls, additional B-channels are opened according to the extra bandwidth setting. For example, if you configure the extra bandwidth setting as 16 Kbps, another B-channel opens when existing bandwidth is reduced to 16 Kbps or less.

Priority reserved bandwidth

The priority reserved bandwidth setting defines how much bandwidth to reserve for high priority stations. The reserved bandwidth cannot be used by stations configured as normal, IP only, or circuit-only priority. High priority stations consume priority reserved bandwidth before consuming unreserved bandwidth.

For example, if you configure the priority reserved setting as 16 Kbps, then only high priority stations can use this reserved bandwidth. When the reserved bandwidth is being used for active high priority calls, additional calls from high priority stations are processed using unreserved bandwidth. If no bandwidth is available, calls to or from high priority stations are blocked until bandwidth becomes available.

Local calling

Introduction

The Remote Office 9150 unit allows you to place calls to other extensions within your office or to telephones in your local community. This is accomplished through the use of up to two local call appearance keys. See Chapter 6, “Using Remote Office 9150 stations,” for a detailed description of the local call appearance keys.

Local extension calling

When you place a call to another telephone in your office using the local call appearance key, it is handled by the Remote Office 9150 unit, not the host PBX.

Note: If the call is initiated from the host call appearance key, then the station-to-station call requires transmission of signaling data through the host PBX.

Local calls through PSTN

The Remote Office 9150 unit allows you to make outgoing and receive incoming PSTN calls over the ISDN BRI connection.

- Make outbound calls by pressing the local call appearance key, and then dialing the trunk access code and the telephone number.
- Answer incoming calls by pressing the flashing local call appearance key.

See Chapter 6, “Using Remote Office 9150 stations,” for a more detailed description of local calling.

Call restrictions

To prevent outgoing calls to certain types of numbers (for example, 1-976), you can disable outgoing calls to specific digit sequences.

Telephone features that are supported

The following Meridian telephone features are supported for local-controlled calls:

- Paging
- Call Waiting
- Hold for calls that appear on local call appearance keys
- Call Transfer (blind and announced) for station-to-station calls only
- Release
- Hands-Free
- calling line identification (CLID) and calling party name display (CPND)

Telephone features that are not supported

The Conference and Call Forward features require a host PBX connection, and, therefore are not supported in local-controlled mode.

Online/offline table

Introduction

The online/offline table is configured on the MIG RLC and allows you to schedule times

- when the ISDN BRI connection to the host PBX is made available to the Remote Office 9150 site

  Note: When the Remote Office 9150 unit is in offline mode, users cannot make or receive calls through the host PBX over the IP or circuit-switched network.
- when all telephones at the Remote Office 9150 site revert to normal telephone service

This allows you to ensure that unwanted ISDN BRI telephone calls through the host PBX are disabled after business hours.

How the table works

You can define 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.

Users at the Remote Office 9150 site can override the settings of the online/offline table, should the table attempt to suspend access to the host PBX in the middle of a business call. Each user station at the remote site is alerted by a buzz and a display message at 30, 20, and 10 seconds before the connection is terminated. To override connection termination, the user must enter the online SPRE code on the telephone.

Configuration

The online/offline table is configured for each remote site on the MIG RLC. Refer to the *Meridian Internet Gateway Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) for configuration information.

For a description of how to go online or offline at the Remote Office 9150 site, see Chapter 6, “Using Remote Office 9150 stations.”

Other supported features

Introduction

This section describes the following additional features supported by the Remote Office 9150 unit:

- fax support
- emergency service number

Fax support

The Remote Office 9150 unit contains one analog port that can be used to send and receive faxes. Faxes can be sent and received in both host- and local-controlled call modes over the IP or circuit-switched network. Faxes are sent uncompressed (that is, 64 Kbps of bandwidth is required).

To support faxing through the host PBX, the fax port on the Remote Office 9150 unit must be associated with a port on the MIG RLC that is configured on the host PBX with data capability.

Emergency service number

If your community has implemented an emergency service number (such as 911) to call the police, fire department, or ambulance, you can configure that number on the Remote Office 9150 unit. This allows users in your office to dial the emergency number and be connected directly to the local emergency dispatch center through the circuit-switched network. The call is automatically routed through the local PSTN without having to dial a local trunk access code.

When you configure the local emergency service number on the Remote Office 9150 unit, you also prevent the call from being automatically routed through the host PBX, which could be in a different city. An emergency call that is routed through the host PBX can result in emergency support being dispatched to the wrong location.

ATTENTION

If you are using only the IP network to route calls, you should make emergency service calls on a telephone that is directly connected to a PSTN line. If you make an emergency service call from a station that is connected to the Remote Office 9150 unit, the call is routed through the host PBX, which could be in a different city.

Administration software

Introduction

Configuration and administration of the Remote Office 9150 unit is performed with the Configuration Manager software, a Windows-based application that is installed on your PC.

The software is provided on the Remote Office Product CD-ROM. You can also obtain it from the Nortel Networks web site.

Administration PC connection options

You can connect the administration PC to the Remote Office 9150 unit through the following:

- an RS-232 connection to the administration PC's serial port
- a 10BaseT Ethernet interface connection

What you can do with Configuration Manager

Configuration Manager allows you to configure the Remote Office 9150 unit. Configuration Manager also provides the Configuration Wizard, which you use for first-time configuration. The Configuration Wizard prompts you for the minimum information that is needed to get the Remote Office 9150 unit communicating with the MIG RLC on the host PBX.

After the initial configuration is completed, use Configuration Manager to administer the Remote Office 9150 unit. Administration tasks include the following:

- viewing the system status
- performing upgrades, backups, or restores
- making configuration changes
- changing the administration password

Command line interface

When the administration PC is connected to the Remote Office 9150 unit through the serial port, you can view the command line interface using an application such as Telnet or HyperTerminal. However, the command line interface is not documented in this guide. Configuration Manager is the supported tool for administering the Remote Office 9150 unit over both the serial port and Ethernet connections.

Chapter 2

Planning for installation

In this chapter

Overview

Introduction

This chapter describes what you must consider when planning to add the Remote Office 9150 product to your IP and telephone networks.

Installation checklist

The installation checklist in this chapter provides a quick reference overview of the tasks required to complete the Remote Office 9150 unit installation and configuration.

Physical environment

Important considerations about the physical environment in which the Remote Office 9150 unit will be installed include

- space requirements and temperature ranges
- mounting options
- cables that are supplied, and cables you must supply yourself

Administration PC

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 Remote Office 9150 unit. It also describes the hardware and software requirements for using the administration software.

Network considerations

The Remote Office 9150 unit communicates through both the IP and the telecommunications networks using a Meridian 1 PBX.

To use the Remote Office 9150 unit in these networks, you must consider the issues described in this chapter.

Trunk management

You can manage connections to the host PBX in several ways:

- Put the Remote Office 9150 unit into offline mode so that it cannot receive or make calls through the host PBX.
- Define a trunk connection as permanent or on-demand.
- Define call duration and idle timers, if the trunk connection is defined as on-demand.
- Define bandwidth allocation settings.
- Use the QoS transitioning technology.

Station configuration

You can configure stations with the ability to make local-controlled calls, host-controlled calls, or both local- and host-controlled calls. If local-controlled call ability is given, specific features can be enabled or disabled.

Security

The Meridian Internet Gateway Reach Line Card (MIG RLC) and Remote Office 9150 unit offer the following types of security:

- security level and, if required, security identifier to prevent toll fraud on the host PBX
- two levels of administration passwords to secure node configurations

The Remote Office 9150 unit does not provide for IP network security. If security on the data network is an issue, you must implement security on the IP network devices.

Deployment options

The MIG RLC on the host PBX and Remote Office 9150 unit can be installed and configured to initially use

- only the IP network (Voice over IP)
- only the circuit-switched network (for example, ISDN BRI trunks)
- both networks (which provides the ability to perform QoS transitions)

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

Gathering the configuration information

To help you plan the configuration of the Remote Office 9150 unit, you can use the Remote Office 9150 forms shown in Appendix B, “Planning forms.”

Future growth

The Remote Office 9150 unit ships with no DSP application or trunk interface modules installed, and provides support for up to

- 32 stations

  Note: You must assign all 32 stations to the same MIG RLC.
- eight simultaneous voice calls over the IP network

You may or may not have purchased DSP application or trunk interface modules to expand its voice processing capability or to use the circuit-switched network.

The Remote Office 9150 unit can change or grow along with your telecommunication needs. This chapter provides planning information for accommodating those needs.

Remote Office 9150

Installation checklist

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

Check	Task	For details, see
❒	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)
❒	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 97.
❒	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"
❒	If you want to use the circuit-switched network to route calls, order trunks from the central office to the Remote Office 9150 unit site. **Note:** The Remote Office 9150 unit supports ISDN BRI trunks (S/T or U interface).	"ISDN BRI information" on page 102.
❒	Obtain the cables that you need to establish the network connections.	"Cables you must supply yourself" on page 74.
❒	Decide on the administration PC setup.	"Administration PC" on page 76.

Remote Office 9150 unit

Installation checklist

Check	Task	For details, see
❒	Gather the configuration information (network addresses, connection numbers, online/offline schedule, QoS thresholds, and so on).	■ "Deployment options" on page 97 ■ Appendix B, "Planning forms"
❒	Install DSP application and trunk interface modules into the Remote Office 9150 unit.	"Installing a trunk interface or DSP application module" on page 116.
❒	Choose a suitable location for the Remote Office 9150 unit.	"Choosing a suitable location" on page 122.
❒	Install the Remote Office 9150 unit in the chosen location.	"Mounting the Remote Office 9150 unit" on page 122.
❒	Connect the Remote Office 9150 unit to the power source, administration PC, and network.	"Connecting the Remote Office 9150 unit" on page 129.
❒	Power up the Remote Office 9150 unit and observe LED behavior. The Status LED remains lit when the power-up cycle completes successfully.	"Powering up the Remote Office 9150 unit" on page 135.
❒	Install the software from the product CD-ROM or the Nortel Networks web site.	"Installing the software" on page 138.
❒	Configure the IP address, subnet mask, and default gateway on the Remote Office 9150 unit.	"Using the Configuration Wizard to perform initial configuration" on page 141.

Remote Office 9150 unit

Installation checklist

Check	Task	For details, see
❒	Configure the following items, as required, to create the communication paths between the Remote Office 9150 unit and the MIG RLC: ■ IP network: MIG RLC's IP address ■ circuit-switched network: ■ MIG RLC's telephone number ■ primary trunk ■ security level and, if required, security identifier	■ "Using the Configuration Wizard to perform initial configuration" on page 141 ■ "Configuring the security level" on page 235
❒	Ping the Remote Office 9150 unit and ensure that it is recognized as a device on the network.	"Testing the network connections" on page 155.
❒	Ensure that the Remote Office 9150 unit's connection information is completed on the MIG RLC.	the *Meridian Internet Gateway Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).
❒	Configure user stations with appropriate calling permissions and features.	"Defining stations" on page 260.
❒	Configure ports on the MIG RLC.	the *Meridian Internet Gateway Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

Remote Office 9150 unit

Installation checklist

Check	Task	For details, see
❒	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 transitioning settings, if required.	■ your data network administrator ■ your telecom network administrator ■ Appendix A, “Network engineering guidelines”
❒	Ensure that calls can be made and received on each station.	“Testing the network connections” on page 155.
❒	Plan for administration training and technical support.	■ Chapter 7, “Administration” ■ Chapter 8, “Troubleshooting”

Physical environment

Introduction

This section provides the space, temperature, cabling, and mounting information you need to know before you install the Remote Office 9150 unit.

Space

Ensure that the Remote Office 9150 unit is installed in a location that is dry and provides plenty of air circulation.

The chosen location should be within cable-length distance from the following:

- the administration PC (if the serial connection is used)
- the Ethernet hub
- trunk and telephone connection interfaces

The Remote Office 9150 unit can be installed up to

- 1230.7 meters (4000 feet) from the digital telephones
- 307.7 meters (1000 feet) from the analog device

It is recommended that you install the Remote Office 9150 unit in the same room where your communications equipment is installed.

Temperature and humidity

The following table describes the temperature and humidity conditions that the Remote Office 9150 unit can withstand without any performance degradation or damage.

Specification	Minimum	Maximum
Normal operation		
Recommended:		
■ Temperature	■ 15°C (59°F)	■ 30°C (86°F)
■ Relative humidity	■ 20%	■ 55% (non-condensing)
Absolute:		
■ Temperature	■ 10°C (50°F)	■ 45°C (113°F)
■ Relative humidity	■ 20%	■ 80% (non-condensing)
Short term (less than 72 hours):	-40°C (-40°F)	70°C (158°F)
Rate of change	Less than 1°C (33.8°F) per 3 minutes	
Storage		
Recommended temperature	-20°C (-4°F)	60°C (140°F)
Relative humidity	5%	95% (non-condensing)
Non-condensing	-40°C (-40°F)	70°C (158°F)
Temperature shock		
In 3 minutes	-40°C (-40°F)	25°C (77°F)
In 3 minutes	70°C (158°F)	25°C (77°F)
Non-condensing	-40°C (-40°F)	70°C (158°F)

Mounting options

You can place the Remote Office 9150 unit on a desk or in a rack, or you can mount it on the wall.

The Remote Office 9150 unit dimensions are

- 42.5 cm (17 in.) wide (without rack-mounting brackets)
- 29.4 cm (11.75 in.) deep
- 4.4 cm (1.75 in.) high

Mounting the Remote Office 9150 unit in a rack

If you want to install the Remote Office 9150 unit in a rack, the rack slot must

- be large enough to provide air circulation to keep the Remote Office 9150 unit cool
- allow you to securely fasten the Remote Office 9150 unit to the rack using the rack-mount brackets

Mounting the Remote Office 9150 unit on the wall

If you want to install the Remote Office 9150 unit on the wall, you can mount it so the cables from the rear panel are directed either right or left. Ensure that the chosen location allows you to easily view the LEDs on the front panel.

ATTENTION

You must complete wall installation using standard telephony installation practices.

Connections

The following connections are made from the rear panel of the Remote Office 9150 unit to the telephone and data networks:

- Two 25-pair connectors (labeled TELCO 1 and TELCO 2) provide tip and ring connections to stations (telephones) and central office trunks (ISDN BRI). These connections provide the interface to the telephone network and the PSTN.

- An RJ-45 connector (labeled ETHERNET) provides a 10BaseT Ethernet connection. This connection provides the ability to pass both voice and data administration traffic over the existing Ethernet network.
- A DB-9 connector (labeled ADMIN) provides an RS-232 serial port connection. You can use this serial port connection to configure a Remote Office 9150 unit that is directly connected to a PC.
- The DB-25 connector (labeled V.35) is for future use.

Cables included with the Remote Office 9150 unit

The Remote Office 9150 unit package includes the following cables:

- power cord and power supply

  Notes:

  - In North America, the power cord and power supply are included inside the Remote Office 9150 box. In all other regions, the power supply is provided inside the box. However, the power cord for your region is provided outside the box.
  - When the North American power cord and power supply are connected together, they are 3.2 meters (10.4 feet) in length.
- RS-232 serial cable

  If the RS-232 cable is not long enough, you can supply your own cable, up to 15.38 meters (50 feet) in length.

Cables you must supply yourself

The cables used to establish the telephone and Ethernet network connections are industry-standard cables. They are not provided in the Remote Office 9150 package. You must obtain them from your local cable supplier.

Telephone network cables

The telephone network cables establish the telephone and trunk connections.

One end of the cable must provide a male 50-pin connector. (This end connects to the Remote Office 9150 unit.)

Ensure that the other end of the cable matches the connectors needed to connect to the telephones or trunks. (For example, if you are using a BIX block to establish the telephone connections, you might need to cut off the connector to expose the wires inside.)

Notes:

- Two telephone cables may be required, based on how many telephones and ISDN BRI lines you plan to connect. (Each telephone cable provides support for up to 16 digital telephones, and two ISDN BRI lines providing two B-channels each. The Telco 1 cable also provides support for one analog station such as a fax machine.)
- Digital telephones should be located no further than 1230.7 meters (4000 feet) from the Remote Office 9150 unit.
- The analog device should be located no further than 307.7 meters (1000 feet) from the Remote Office 9150 unit.

Ethernet cable

If you are connecting the Remote Office 9150 unit to a hub, you need a standard CAT5 unshielded twisted-pair (UTP) straight-through Ethernet cable. The cable should be no longer than 100 meters (325 feet) in length.

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 Remote Office 9150 unit. It also describes the hardware and software requirements for using the administration software.

Connection options

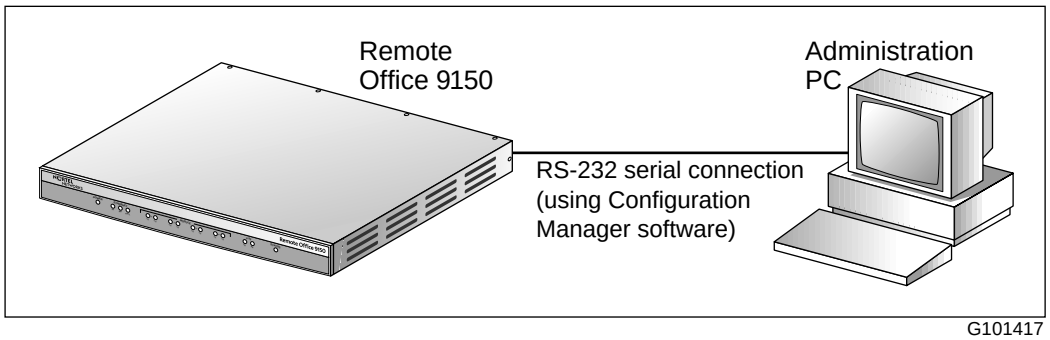
The Remote Office 9150 product includes the Configuration Manager software that enables you to configure, administer, and upgrade the Remote Office 9150 unit. You can perform these tasks over one of the following:

- an RS-232 serial connection (required for first-time configuration only)
- a 10BaseT Ethernet connection (for ongoing administration and upgrades)

Serial connection

You must use the serial connection when you first install and configure the Remote Office 9150 unit. You must establish a serial connection to the Remote Office 9150 unit to enter the IP interface information.

See the following diagram.



G101417

You can continue using the serial connection for ongoing administration of the Remote Office 9150 unit, if you wish. However, if this is the only connection option used, you cannot administer the Remote Office 9150 unit remotely or perform upgrades.

Note: When the administration PC is connected to the Remote Office 9150 unit through the serial port, you can view the command line interface using an application such as Telnet or HyperTerminal. However, the command line interface is not documented in this guide. Configuration Manager is the supported tool for administering the Remote Office 9150 unit over the serial port.

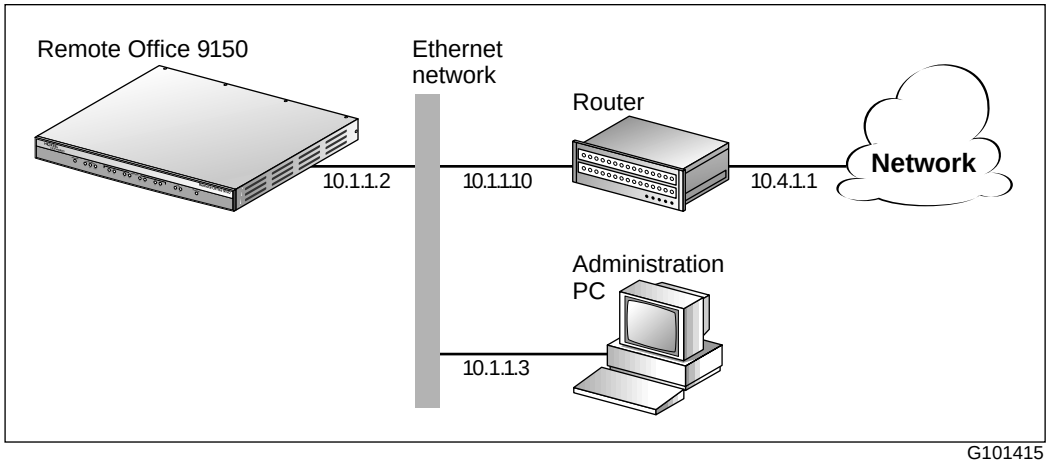
Ethernet connection

Once you configure the Remote Office 9150 unit with its IP interface information, the following can happen:

- Communication can be established between the Remote Office 9150 unit and the MIG RLC (that is, calls can be routed over the IP network).
- You can administer and upgrade the Remote Office 9150 unit over the IP network.

  This means you do not have to install an administration PC in the same location as the Remote Office 9150 unit.

See the following diagram.

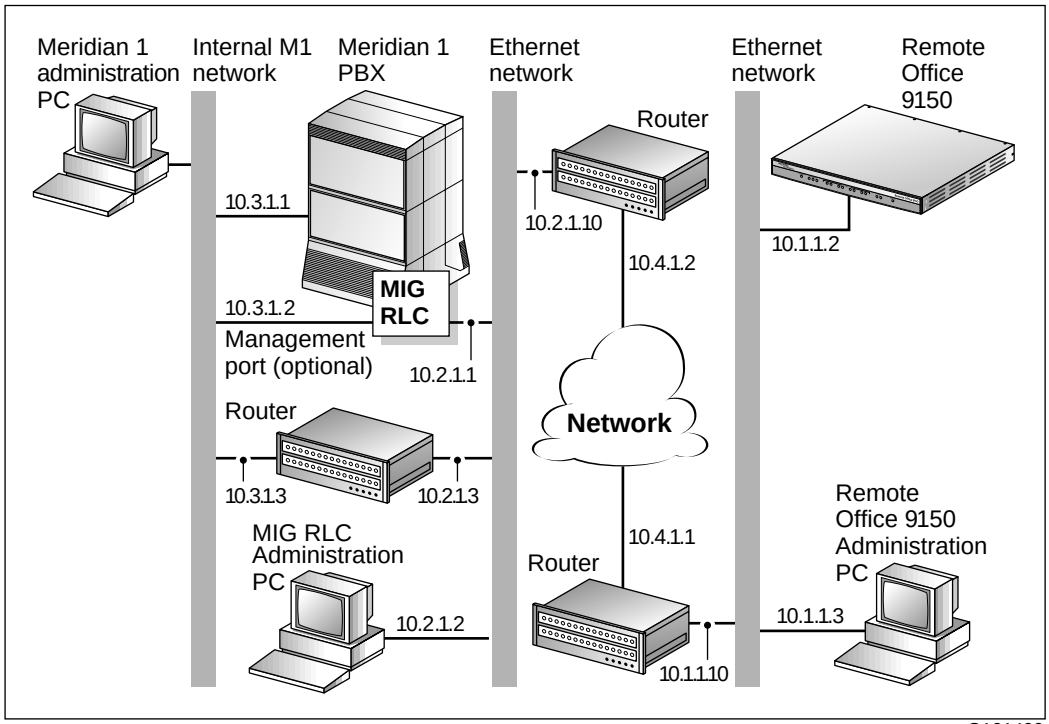


G101415

Administering multiple nodes in the network

If you are responsible for administering one or more Remote Office 9150 units and the MIG RLC on the host PBX, you can access the Remote Office 9150 unit and the MIG RLC 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 the Remote Office 9150 unit. You can use one administration PC to administer all units in the Remote Office network.



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 wish to use the RS-232 serial port to establish a direct serial connection
- be equipped with a pointing device (mouse)
- 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 Trivial File Transfer Protocol (TFTP) server application installed to perform firmware upgrades and configuration uploads.

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

Year 2000 compliance

The Remote Office 9150 unit and Configuration Manager software are Year 2000 compliant. However, you must ensure that 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 or higher
Windows 95	Version 95b

Operating system	Year 2000 compliance requirement
Windows 98	OK as is

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 operation of these two applications on the same PC has not been tested and therefore, is not supported.

Network considerations

Introduction

The Remote Office 9150 unit communicates through both the IP and telecommunications network using a Meridian 1 PBX.

To use the Remote Office 9150 unit in these networks, you must consider the issues described in this section.

IP addressing and routing

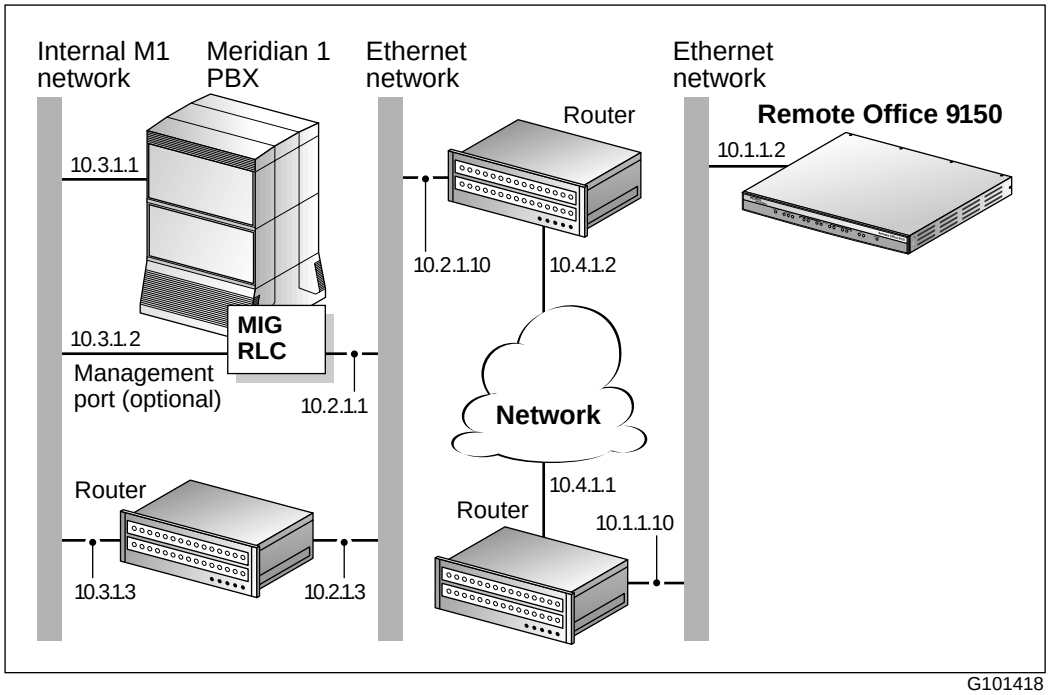
To make and receive calls over the IP network, the Remote Office 9150 unit must be

- physically connected to the IP network
- assigned a subnet mask, default gateway, and unique IP address

  Note: Similarly, a subnet mask, gateway, and unique IP address must be assigned to the MIG RLC on the host PBX.
- able to send and receive traffic to and from the MIG RLC on the host PBX

Network diagram

The following diagram shows the Remote Office 9150 unit's position in an IP network.



Note: For placement of one or more administration PCs, see "Administration PC" on page 76.

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 subjected to many delays, voice quality is affected.

For more information, see Appendix A, "Network engineering guidelines."

Numbering plans

Each trunk groups at the Remote Office 9150 unit site must be assigned a trunk access code (that is, the number dialed to obtain an outgoing trunk). In addition, special prefix (SPRE) codes must be defined for the following features if you want to use them:

- paging
- local calling on ATA-equipped analog devices
- to go online or offline (for more details, see “Online/offline table” on page 57)
- registration and deregistration for multi-user or dynamic ports

All trunk access and SPRE codes are automatically defined in Configuration Manager with a pound prefix (# in North America) so that there are no conflicts with host PBX dialing plans. For a list of the default trunk access and SPRE codes, refer to the “Remote Office 9150 Configuration Information—Dialing Plans” form on page 436.

Numbering plan for local stations

You should consider the numbering plan on the host PBX when setting up the numbering plan for local stations at the Remote Office 9150 unit site. This ensures that station-to-station calls through the host PBX complete correctly.

Call blocking

Call blocking can occur when there are more users installed and more calls being processed than can be supported by the Remote Office 9150 unit’s DSP application and trunk interface modules.

The voice processing capacity of the Remote Office 9150 system depends on the number of DSP application and trunk interface modules installed in the Remote Office 9150 unit and the amount of bandwidth available to process calls. If bandwidth is not available, additional calls are blocked. (This setting is configured on the MIG RLC for each site). This voice processing capacity defines how many calls can be active at one time.

The Remote Office 9150 unit ships with the ability to support up to 32 users, with up to 8 simultaneous calls (providing a 4:1 call blocking ratio). By adding additional DSP application or trunk interface modules, you can reduce or eliminate call blocking.

Reducing call blocking between the Remote Office 9150 unit and the host PBX

Each DSP application module provides the ability to support eight more simultaneous calls when voice traffic is routed over the IP network. Up to three more DSP application modules can be installed in the Remote Office 9150 unit, allowing 32 active calls at one time.

Note: If you add DSP capacity to the Remote Office 9150 unit, you must add the same DSP capacity to the MIG RLC on the host PBX.

Trunks are required for the Remote Office 9150 unit to operate in circuit-switched mode (that is, over the PSTN instead of the IP network). Trunks are used to route calls between the Remote Office 9150 unit and the host PBX or the local PSTN.

By default, the Remote Office 9150 unit ships with no trunks installed. Trunks can be provided by installing trunk interface modules.

The number of trunks you can install depends on the type of trunk interface modules used on the Remote Office 9150 unit. For example, if ISDN BRI trunks are used, each trunk interface module provides one BRI trunk (providing two B-channels). You can install up to four trunk interface modules in the Remote Office 9150 unit.

Note: The Remote Office 9150 unit supports only ISDN BRI S/T or U trunks.

Calculating system requirements

To determine how many DSP application or trunk interface modules are needed to reduce or eliminate call blocking, use the “Remote Office 9150 System expansion worksheet” on page 437.

Managing trunk connections

Introduction

You can manage trunk connections to the host PBX in several ways:

- Put the Remote Office 9150 unit into offline mode, so that it cannot receive or make calls through the host PBX when operating in circuit-switched mode.
- Define a trunk connection as permanent or on-demand.
- Define call duration and idle timers, if the trunk connection is defined as on-demand.
- Define minimum and maximum bandwidth allocation settings.
- Use the QoS transitioning technology.

Quality of Service transitioning technology

On IP networks, traffic congestion or delays can occur that result in poor voice quality or lost connections. The MIG RLC can be configured to transition call processing from the IP network to the circuit-switched network when the Quality of Service degrades. When Quality of Service on the IP network returns to normal, call processing can be transitioned back to the IP network.

The points at which the transition occurs are determined by the Quality of Service thresholds (level and duration) defined on each MIG RLC port. To determine appropriate thresholds for each site in your network, you should consult your data network administrator. For more information, see Appendix A, “Network engineering guidelines.”

Online/offline schedule

You can configure an online/offline schedule on the MIG RLC to control when the Remote Office 9150 unit can make and receive calls through the host PBX. When the Remote Office 9150 unit is in offline mode, calls cannot be made or received through the host PBX over the IP or circuit-switched network.

You should configure offline entries

- for times when the connection to the host PBX should not be active, such as during evenings and weekends
- to prevent the Remote Office 9150 unit from staying online permanently, thereby eliminating unwanted ISDN BRI charges

When the MIG RLC processes an offline entry, it instructs the Remote Office 9150 unit to go offline for a specified number of hours and minutes. The number of hours and minutes the Remote Office 9150 unit 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 following day. When the MIG RLC processes the 6:00 p.m. entry, it instructs the Remote Office 9150 unit to go offline for 15 hours.

When going offline, a timer is activated within the Remote Office 9150 unit. When the timer expires (in the example above, at 9:00 a.m.), the Remote Office 9150 unit automatically initiates a “going online” request to the host PBX. If the MIG RLC successfully receives the request, the Remote Office 9150 unit and its connected telephones go online.

Changing the online/offline mode

Whether an online/offline schedule is used or not, you can put the Remote Office 9150 unit into online or offline mode at any time by dialing the online or offline SPRE code at any phoneset connected to the Remote Office 9150 unit. The SPRE codes are configured on the Remote Office 9150 unit.

Trunk connection type and timers

On the Remote Office 9150 unit, you can define each trunk as a permanent or on-demand connection. When the trunk is defined as an on-demand connection, the trunk is activated only when a call is received from the host PBX, or initiated by a user at the Remote Office 9150 site. You can reduce connection charges by defining trunks as on-demand connections.

When you define a trunk as on-demand, you can further reduce connection charges by configuring call duration and idle timers. These timers are configured on the MIG RLC for your site.

Trunk bandwidth allocation

The Remote Office 9150 unit can dynamically allocate available trunk bandwidth to active calls in circuit-switched mode. As calls are initiated and bandwidth requirements increase, additional trunk connections are established. Similarly, as calls terminate and bandwidth requirements drop, calls are aggregated and idle trunks are shut down.

Station configuration

Introduction

When planning the stations at the Remote Office 9150 site, you must think about the call capabilities required by each station.

Each station at the Remote Office 9150 site inherits settings such as voice compression and priority from the MIG RLC port with which it is associated. At the Remote Office 9150 site, the station is configured with the ability to make local-controlled calls, host-controlled calls, or both local- and host-controlled calls. For stations defined with local- or local- and host-controlled capability, specific features can be enabled or disabled.

MIG RLC settings

You must define the following on each MIG RLC port:

- port allocation as dedicated, multi-user, or dynamic
- whether voice compression will be used
- priority level

Port allocation

Assign each user at the Remote Office 9150 site to one port on the MIG RLC on the host PBX. You can configure MIG RLC port in one of the following ways:

- as a dedicated port (one port per remote user)
- as a multi-user port (one port shared by multiple users)

  Up to eight persons can share the same MIG RLC port, but not at the same time. All stations that use this type of port must respond to the same DN and have identical phoneset configurations. This port type is especially useful for employees who are working in mutually exclusive shifts.

- as part of a dynamic pool

  Dynamic port pooling is similar to a multi-user port except that the persons who share ports in a dynamic pool are assigned to the next available port in the MIG RLC port pool. There is no correlation between the station and the port on the MIG RLC.

  This feature is especially useful in free-seated ACD environments where agents log on to the host PBX using their agent IDs.

Voice compression

If calls are to be routed over the IP network, you must select one of the following voice compression algorithms on each MIG RLC port:

- G.711: Voice is transmitted at 64 Kbps (no compression).
- G.726: Voice is compressed and transmitted at 32 Kbps.
- G.729A: Voice is compressed and transmitted at 8 Kbps.

  G.729A is the default voice compression algorithm used by the MIG RLC. This allows

  - up to six simultaneous voice calls to be processed over the first ISDN BRI B-channel (16 Kbps are reserved for signaling data)
  - up to eight simultaneous voice calls to be processed over the remaining ISDN BRI B-channels

Each Remote Office 9150 station inherits its compression algorithm from the MIG RLC port to which it has been assigned.

Station priority

You can configure each MIG RLC port that is assigned to each station as normal priority, high priority, circuit-switched only, or IP only.

When the port is configured as high priority and the priority reserved setting is configured on the connection between the MIG RLC and Remote Office 9150 unit, you can ensure voice Quality of Service for calls to and from those stations.

For more details, see “Station priority” on page 52 and “Connection bandwidth” on page 54.

Notes:

1. Each Remote Office 9150 station inherits its priority setting from the MIG RLC port to which it has been assigned.
2. The number of MIG RLC ports that you can configure as high priority depends on the amount of available bandwidth. The MIG RLC administrator must ensure that enough bandwidth is available to process calls on normal priority ports.

Remote Office 9150 settings

You can define the following settings for each Remote Office 9150 station:

- port type as local, remote, or both
- extension (directory) number (on local stations only)
- key placement (on local stations only)

Port types

On the Remote Office 9150 unit, you can define each station with one of the following capabilities:

- local control only (local)

  You can use stations defined as *local* to make and receive calls through the local PSTN. You can also make station-to-station calls at the Remote Office 9150 site. Calls through the host PBX are not allowed.

- host control only (remote)

  If a particular station is not allowed to make or receive calls through the local PSTN, that station is configured as *remote* only. All calls are routed through the host PBX, except for emergency calls (such as 911). If the emergency service number is configured on the Remote Office 9150 unit, calls made to the emergency number are routed through the local PSTN so the emergency service receives the correct location information.

- both local and remote control

  You can use stations defined as *local and remote* to make and receive calls through both the host PBX and the local PSTN. You can also make station-to-station calls at the Remote Office 9150 site.

Outgoing calls are routed according to the call appearance key used to initiate the call. Calls initiated on the key defined as the primary or host call appearance key are routed through the host PBX. Calls initiated on the key defined as the local call appearance key are routed through the local PSTN, if a trunk access code was dialed before the telephone number.

When a station is configured with local control capability, further configuration of the station is required to

- enable or disable certain features
- disable outgoing calls or single-digit dialing, if required
- define key placement on the telephone

User extension configuration

Each station is assigned a local directory number (DN). The Remote Office 9150 unit uses the DN to route the incoming call to the correct station.

Stations that are configured with host-controlled call capability are associated with a port number on the MIG RLC. The MIG RLC and the Remote Office 9150 unit use this port number to establish the communication path between the host PBX and the station.

Placement of local call appearance and feature keys

When determining the placement of the local call appearance key on a station, ensure that the key position is not already configured for a specific feature on the host PBX. If you configure a PBX-configured feature key as a local call appearance key, the user cannot use that feature.

If the station is configured with local control capability, you can also configure the placement of other keys, such as Transfer, Call Waiting, and Make Set Busy.

Security

Introduction

The MIG RLC and Remote Office 9150 unit offer the following types of security:

- security level and, if required, security identifier to prevent toll fraud on the host PBX
- two levels of administration passwords to secure node configurations

Toll fraud

You can minimize toll fraud on the PBX by implementing one of the following levels of security:

- Caller ID

  When Caller ID is selected, the Remote Office 9150 unit's calling line identification (CLID) is compared with its PSTN number configured on the MIG RLC port when a connection to the host PBX is attempted. If they match, the connection is established. If they do not match, the host PBX drops the call.

  Caller ID authentication cannot be performed over the IP network.

- security identifier

  You can use security identifier authentication over the IP or circuit-switched network. If this level is chosen, a security identifier must be configured on both the Remote Office 9150 unit and the MIG RLC port to which the unit is assigned. When a connection between the host PBX and Remote Office 9150 unit is attempted, the security identifiers are compared. If they match, the connection is established. If they do not match, the host PBX drops the call.

Data network security

The Remote Office 9150 solution does not provide for data network security. If security on the data network is an issue, security must be implemented on the data network devices.

System configuration

The MIG RLC and Remote Office 9150 unit configurations are protected by two layers of security:

- administration password

  The administration password is required when starting the Configuration Manager software. If the password is not known, the person attempting to use the Configuration Manager cannot log on to any Remote Office node.

  Note: A node is any MIG RLC or remote site connected to the MIG RLC.

- node password

  The node password is required before the configuration of a particular node can be displayed or modified.

Planning for future growth

Introduction

The Remote Office 9150 unit can change or grow along with your telecommunication needs. This section describes planning for accommodating those needs.

Adding DSP modules

The Remote Office 9150 unit ships with the ability to support up to 32 stations (which must all be assigned to one MIG RLC). Up to eight simultaneous voice calls can be supported when calls are routed over the IP network.

You can increase the voice processing capability of the Remote Office 9150 unit by installing up to three more DSP modules. Each DSP module adds support for up to eight more simultaneous calls (to a maximum of 32).

To determine how many DSP application modules you need to install, use the “Remote Office 9150 System expansion worksheet” on page 437. For instructions on installing additional DSP modules, see “Installing a trunk interface or DSP application module” on page 116.

Note: When installing additional DSP modules on the Remote Office 9150 unit, you must also increase voice processing capability in a similar manner on the MIG RLC. The number of modules that need to be added on the MIG RLC depend on the requirements of other remote units connecting to the same MIG RLC. If only this Remote Office 9150 unit is connecting to the MIG RLC, then the same number of DSP modules must be installed on both the Remote Office 9150 unit and the MIG RLC. To calculate the MIG RLC’s DSP requirements, use the “Meridian Internet Gateway Reach Line Card System expansion worksheet” on page 458.

Adding trunk interface modules

Initially, the Remote Office 9150 unit ships with no trunks. As connection needs change, you can add up to four ISDN BRI S/T or U trunk interface modules.

To determine how many trunk interface modules you need to install, use the “Remote Office 9150 System expansion worksheet” on page 437. For instructions on installing or replacing existing trunk interface modules, see “Installing a trunk interface or DSP application module” on page 116.

Maximum configurations

The following table identifies the maximum configurations for the Remote Office 9150 solution:

Component	Maximum
MIG RLC connections	1 **Note:** You must assign all users at the Remote Office 9150 site to the same MIG RLC.
DSP application modules	3
ISDN BRI modules	4
ISDN BRI lines	4 **Note:** Each line is associated with one ISDN BRI module and provides two B-channels.
Trunk groups	10
Digital telephones	32
Analog telephone or fax machine	1
MCAs or ATAs	■ 4 if the Remote Office 9150 unit is connected to a 1-slot MIG RLC (supporting 16 users). ■ 7 if the Remote Office 9150 unit is connected to a 2-slot MIG RLC (supporting 32 users).

Component	Maximum
MCAs or ATAs (continued)	**Notes:** ■ You can have eight MCAs or ATAs installed if an analog telephone or fax machine is *not* installed. ■ The total number of digital telephones and ATAs cannot exceed 32.

Deployment options

Introduction

You can install and configure the MIG RLC on the host PBX and Remote Office 9150 unit to initially use

- only the IP network (Voice over IP)
- only the circuit-switched network (for example, ISDN BRI trunks)
- both networks (which provides the ability to perform QoS transitions)

If you choose not to use both networks initially, this section suggests how you can gradually phase in Voice over IP and QoS transition 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 Remote Office 9150 unit and MIG RLC. This allows you to administer both 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 user station assignment. For this release, each user at the Remote Office 9150 site must be assigned to one MIG RLC port that is configured on the host PBX with voice capability.

Exception: You must assign the fax machine and stations that use ATAs or MCAs for data transmission to ports that are configured on the host PBX with data capability.

If the circuit-switched network will be used to route calls, one data port on the host PBX must be dedicated to the Remote Office 9150 site to establish the call connections.

Use the following forms to plan port and station assignment:

- “Remote Office 9150 Configuration Information—Stations” on page 428
- “Meridian Internet Gateway Reach Line Card Connection Information—16 ports” on page 444
- “Meridian Internet Gateway Reach Line Card Connection Information—32 ports” on page 449

To implement circuit-switched mode

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

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

To use this scenario, follow these steps:

1 Determine how many simultaneous calls you want to process over the circuit-switched network. This will help you determine how many trunk interface modules and DSP application modules to install on the Remote Office 9150 unit.

To do this, complete the “Remote Office 9150 System expansion worksheet” on page 437.

Similarly, you must calculate how many DSP application modules to install on the MIG RLC (if any), using the “Meridian Internet Gateway Reach Line Card System expansion worksheet” on page 458.

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

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

Similarly, install DSP application modules on the MIG RLC, if needed.

Note: The Remote Office 9150 unit does not ship with trunk interface modules or DSP application modules installed. The MIG RLC does not ship with DSP application modules installed.

4 Obtain the ISDN BRI information for each line from the Remote Office 9150 site's PSTN service provider. This information must be configured on the Remote Office 9150 unit.

5 Identify the telephone number assigned to the B-channel that will be used as the primary trunk connection to the MIG RLC on the host PBX. This telephone number must be configured on the MIG RLC, and is used by the MIG RLC to establish connections with the Remote Office 9150 unit.

6 Similarly, obtain the telephone number assigned to the MIG RLC port to which this Remote Office 9150 unit is assigned. This telephone number must be configured on the Remote Office 9150 unit, and is used by the Remote Office 9150 unit to establish connections with the MIG RLC.

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 the 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 in host-controlled mode, follow these steps

1 Determine how many simultaneous calls you want to process. This will help you determine how many DSP application modules to install on the Remote Office 9150 unit. To do this, complete the "Remote Office 9150 System expansion worksheet" on page 437.

Similarly, you must calculate how many DSP application modules to install on the MIG RLC (if any), using the "Meridian Internet Gateway Reach Line Card System expansion worksheet" on page 458.

2 Install DSP application modules on the Remote Office 9150 unit, if needed. Up to three DSP application modules can be installed.

Similarly, install DSP application modules on the MIG RLC, if needed.

3 Obtain an IP address assigned for the Remote Office 9150 unit. This IP address must be configured on the MIG RLC, and is used by the MIG RLC to establish connections with the Remote Office 9150 unit.

4 Similarly, obtain the IP address assigned to the MIG RLC. This IP address must be configured on the Remote Office 9150 unit, and is used by the Remote Office 9150 unit to establish connections with the MIG RLC.

5 If 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

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

To implement the Quality of Service transitioning technology

When the QoS transitioning technology is implemented, calls transition

- to the circuit-switched network when IP QoS degrades
- back to the IP 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 is processed (during normal and busy traffic periods)
- how to evaluate and adjust your network's Quality of Service

For more details, consult with your data network administrator and refer to Appendix A, "Network engineering guidelines."

2 Once you have this information and understand it, determine what the QoS settings should be, and then configure them on each MIG RLC port.

For instructions, refer to the *Meridian Internet Gateway Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

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 Quality of Service is acceptable.

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

Planning the configuration

Introduction

Before you configure the Remote Office 9150 unit, it is strongly recommended that you complete the data entry forms shown in Appendix B, “Planning forms.”

This section describes the information you can configure on the Remote Office 9150 unit.

Data entry form completion sequence

You should complete the data entry forms in the following sequence:

1. Remote Office 9150 Configuration Information—Stations form
2. Remote Office 9150 Configuration Information—ISDN BRI Modules form
3. Remote Office 9150 Configuration Information—Network Connections form
4. Remote Office 9150 Configuration Information—Dialing Plans form

For more details, see Appendix B, “Planning forms.”

Station assignments and configuration

You must assign each telephone in your office to one of the 32 ports provided by the Remote Office 9150 unit. You can configure stations with the ability to make local-controlled calls (local), host-controlled calls (remote), or both (local and remote).

If a station will be configured with the ability to make host-controlled calls, then that station is mapped to a MIG RLC port (which, in turn, is mapped to telephone port configuration on the host PBX).

If a station will be configured with the ability to make local-controlled calls (including station-to-station dialing), you must take the numbering plan on the host PBX into consideration. You need to ensure that when users dial another station in the same office in host-controlled mode, the call routes correctly.

Stations that will be used for local-controlled calls can be further configured with features and their key locations.

ISDN BRI information

Providing information to your service provider

To ensure that you get the correct ISDN service for the Remote Office 9150 unit, tell your service provider how the ISDN line should be provisioned. Request the following:

- two B-channels providing voice and data capability

  Both B-channels must be Circuit Switched Voice and Data.

- Calling Line Identification (CLI) or Caller ID

  CLI provides the caller's telephone number when you receive a call. This information is provided by the network and not the caller, so it can be used as a security measure to identify calls to be accepted and rejected.

- 64 Kbps clear channel

  Note: A 64 Kbps clear channel is also required on the ISDN PRI connection between the host PBX and the PSTN. A 56 Kbps channel does not provide enough bandwidth to process one call using G.711 compression.

Receiving information from your service provider

In return for providing the ordering information, your service provider gives you directory numbers and, if used in your area, Service Profile Identifiers (SPIDs). SPIDs are not provided for the AT&T 5ESS Custom service.

A directory number is the address or ISDN telephone number for the ISDN line assigned by the service provider. Each ISDN line receives at least one telephone number, called the Primary Directory Number.

If used in your area, your service provider provides you with the SPIDs. These are associated with the service you have ordered, and you must use these as part of the configuration for the Remote Office 9150 unit before any ISDN connections can be made (except for AT&T Custom). The SPID is similar to the ISDN telephone number and its format is unimportant as long as the information is entered correctly when configuring the Remote Office 9150 unit.

IP addresses

If you want to administer the Remote Office 9150 unit over the IP network, the following information is required for the Remote Office 9150 unit:

- IP address (it must be unique)
- subnet mask
- default gateway

If you want to route voice traffic over the IP network, you also need the MIG RLC's IP address. The Remote Office 9150 unit uses these IP addresses to establish the connection with each other.

Connection between the MIG RLC and Remote Office 9150 unit information

If you want to route voice traffic over the circuit-switched network, the telephone numbers for each end of the network are required. If security is being implemented, the security authentication information (Caller ID or security identifier) is also needed.

Online/offline schedule

You can configure each port on the MIG RLC with a schedule that identifies when a remote site is online (connected to the corporate PBX) or offline. When the Remote Office 9150 unit is in offline mode, calls cannot be made or received through the host PBX over the IP or circuit-switched network.

You can configure only one online/offline schedule for the MIG RLC port. This schedule affects all stations at the Remote Office 9150 site. You should create offline entries

- for times when the connection to the host PBX should not be active, such as during evenings and weekends
- to prevent the Remote Office 9150 unit from staying online permanently, thereby eliminating unwanted ISDN BRI charges

To help you plan the online/offline schedule configuration on the MIG RLC, use the "Meridian Internet Gateway Reach Line Card Online/Offline Table Configuration" form on page 457.

Trunk configuration information

Trunk configuration on the Remote Office 9150 unit consists of defining the ISDN BRI lines from the central office and assigning one or more B-channels, if desired, to trunk groups.

Numbering plan

You must assign a trunk access code to each trunk group at the Remote Office 9150 unit site. A trunk access code is the number that must be dialed to obtain an outgoing trunk. In addition, you must define special prefix (SPRE) codes for the following features if you want to use them:

- paging
- to go online or offline (for more details, see "Online/offline table" on page 57)
- local calling

  This allows analog or ATA-equipped station users to change the outgoing call mode to local-controlled mode. (Host-controlled mode is the default mode when users go offhook on analog or ATA-equipped stations.)
- registration and deregistration

  The registration SPRE code is used to register the station user with a multi-user or dynamic port.

  The deregistration SPRE code disengages the user from the port so that another user can use it. The user is put into *not logged in* mode.

All trunk access and SPRE codes are automatically defined in Configuration Manager with a pound sign (# in North America) so that there are no conflicts with host PBX dialing plans. The maximum length of each code is three digits in addition to the pound sign. For a list of the default SPRE and trunk access codes, refer to the "Remote Office 9150 Configuration Information—Dialing Plans" form on page 436.

Note: You can change the defaults if you wish.

Chapter 3

Installing the Remote Office 9150 unit

In this chapter

Overview

Introduction

This chapter explains how to install the Remote Office 9150 unit in your office.

Safety

This document contains general safety guidelines that are recommended by Nortel Networks. You must follow these safety guidelines whenever you perform installation or maintenance tasks on the Remote Office 9150 unit.

This guide provides warnings when risks related to hardware installation and handling are known. For a description of the types of warnings this guide provides, see “Conventions used in this guide” on page xxii. Do not ignore these warnings.

Tools

Ensure you have the tools necessary for completing hardware and software installation and configuration. These include

- the tools listed on page 110
- data entry forms located in Appendix B, “Planning forms”

Hardware installation

The hardware installation procedures described in this chapter include

- installing DSP application or trunk interface modules when needed (to include call processing capability)
- installing the Remote Office 9150 unit
  - on a desk
  - on a wall
  - in a rack

- connecting the Remote Office 9150 unit to the
  - power source
  - telephones and ISDN BRI trunks
  - Ethernet network
  - administration PC
- powering up the Remote Office 9150 unit

Software configuration

The Configuration Manager software is used to configure and administer the Remote Office 9150 unit. This software is located on the CD-ROM provided in the package. You must install the software on the administration PC.

After the software is installed, you must

- start the software
- connect to the Remote Office 9150 unit through the serial port
- run the Configuration Wizard to configure the minimum information needed to route traffic between the Remote Office 9150 unit and the MIG RLC on the host PBX
- perform tests to verify that the system is working

General safety

Introduction

This section describes the general safety guidelines recommended by Nortel Networks. You must follow these safety guidelines whenever you perform installation or maintenance tasks on the Remote Office 9150 unit.

Precautionary messages

This guide provides warnings when risks related to hardware installation and handling are known. For a description of the types of warnings this guide provides, see “Conventions used in this guide” on page xxii. Do not ignore these warnings.

Safety precautions

To avoid damage or injury, follow these safety precautions at all times.

Plug the Remote Office 9150 unit into a properly grounded power source to reduce the possibility of electric shock and damage to the unit or network.

DANGER

Risk of electric shock

Disconnect the power as well as the Telco 1 and Telco 2 cables before you perform any hardware troubleshooting or add ISDN BRI or DSP application modules to the Remote Office 9150 unit.

If you do not disconnect the Telco 1 and Telco 2 cables from the Remote Office 9150 unit, you can receive a lethal shock if an external telco line is accidentally severed.

Ensure that nothing rests on connection cables, and that cables cannot be tripped over or stepped on.

Electrostatic discharge safety precautions

Electrostatic discharge (ESD) affects the performance and decreases the useful life of system components. ESD can seriously damage component parts, such as circuit cards.

Implement the following 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. (For example, wear an antistatic wrist strap attached to any unpainted metal surface that is connected to an electrical ground.)

Required tools

Introduction

This section identifies the tools you need to perform Remote Office 9150 unit installation and maintenance tasks.

Hardware installation tools

You need the following tools to install the Remote Office 9150 unit, or to install or replace DSP application or trunk interface modules:

- an antistatic ESD wrist strap (recommended)
- a Phillips (cross-head) screwdriver
- a pen or pencil for
  - noting the installation location (if mounting on a wall)
  - noting cable lengths
  - labeling cables
- cable tie wraps
- cable identification labels
- a tape measure
- four wood screws if you want to mount the Remote Office 9150 unit on the wall

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 PC with a CD-ROM drive or an Internet connection for obtaining software, firmware, and documentation updates
- a TFTP server application installed on the PC

  The TFTP server is required for performing firmware upgrades. If a TFTP server is currently not installed, you can obtain one from the Internet.

Unpacking and inspecting the equipment

Introduction

Before you install the Remote Office 9150 unit, ensure that the package contents are all present and are not damaged.

Before you begin

Before you unpack the equipment, ensure that your work area is safe from electrostatic discharge. For more details, see “Electrostatic discharge safety precautions” on page 109.

To inspect the package contents

1. Inspect the box in which the Remote Office 9150 unit was shipped for damage.
2. Open the box and remove its contents.
3. Verify that, in addition to this guide, the following items are present:

Check	Item
❒	Remote Office 9150 unit
❒	Package containing rubber feet and rack-mounting brackets with screws
❒	Power cord and power supply **Note:** In North America, the power cord and power supply are included inside the Remote Office 9150 box. In all other regions, the power supply is provided inside the box and the power cord for your region is provided outside the box.
❒	RS-232 serial cable

Check	Item
❒	*Remote Office and MIG RLC Release Notes* (NTP 555-8421-102)
❒	*Remote Office Product CD-ROM*

4 Visually inspect each item for obvious faults or damage.

What to do if damage is found

If any component is damaged, report the damage immediately to your Nortel Networks distributor and the carrier who delivered the equipment.

What's next?

When you have verified that all components are present and are undamaged, do the following:

- Install DSP application and trunk interface modules, if required.

  For instructions, see "Installing a trunk interface or DSP application module" on page 116.

- Install the Remote Office 9150 unit in its chosen location.

  For instructions, see "Mounting the Remote Office 9150 unit" on page 122.

Removing the Remote Office 9150 unit cover

Introduction

As you increase or change the voice processing capability of the Remote Office 9150 unit, you need to perform one or more of the following tasks:

- Install additional trunk interface modules.
- Install additional DSP application modules.

To perform these tasks, you must remove the Remote Office 9150 unit cover.

To remove the Remote Office 9150 unit cover

DANGER

Risk of electric shock

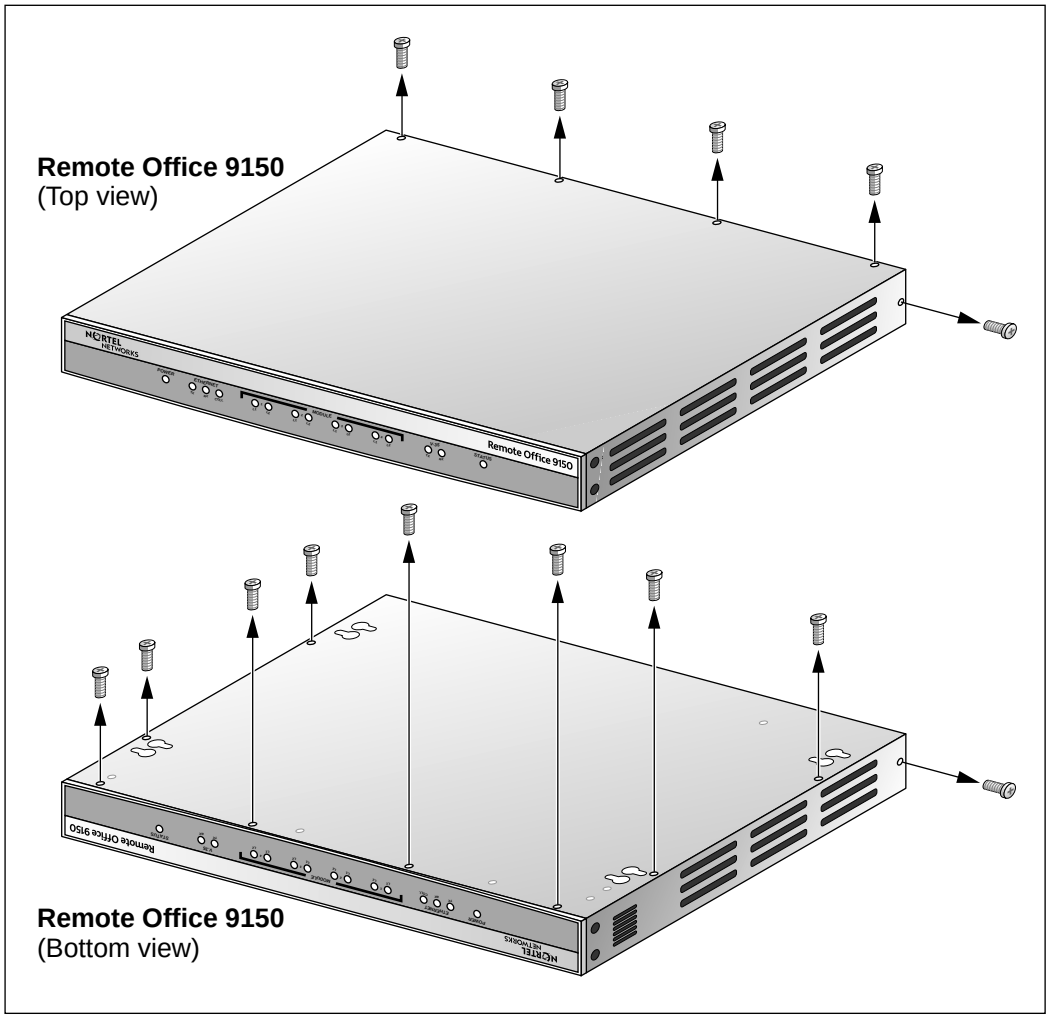
Disconnect the power as well as the Telco 1 and Telco 2 cables before you perform any hardware troubleshooting or add ISDN BRI or DSP application modules to the Remote Office 9150 unit.

If you do not disconnect the Telco 1 and Telco 2 cables from the Remote Office 9150 unit, you can receive a lethal shock if an external telco line is accidentally severed.

1 Use a Phillips screwdriver to remove the following screws from the Remote Office 9150 unit cover:

- two screws from the sides
- four screws from the top
- eight screws from the bottom

See the diagram on page 114.


Remote Office 9150
(Top view)
Remote Office 9150
Remote Office 9150
(Bottom view)

G101406

2 Place the screws in a safe place where they cannot be lost.

3 Ensure the Remote Office 9150 unit is placed top side up.

4 Remove the cover as follows:

   a. Grasp both sides of the Remote Office 9150 unit.

   b. Slide the cover toward you.

   c. Lift the cover off the unit.

   d. Put the cover aside.

5 Turn the Remote Office 9150 unit so the rear panel faces you.

6 This allows you to read the labels on the Remote Office 9150 unit circuit board.

7 Perform module installation as required.

   For instructions, see “To install a trunk interface or DSP application module” on page 119.

8 Replace the cover as described in “To replace the Remote Office 9150 unit cover” below.

To replace the Remote Office 9150 unit cover

1 Carefully slide the top cover into position over the circuit board so that the holes along the top edge of the rear panel are aligned.

2 Replace the four screws on the top.

3 Replace the two screws on the sides.

4 Turn the Remote Office 9150 unit over and replace the eight screws on the bottom.

5 Continue with “Mounting the Remote Office 9150 unit” on page 122.

Installing a trunk interface or DSP application module

Introduction

The Remote Office 9150 unit ships from Nortel Networks with

- no trunk interface modules installed
- one Digital Signal Processor (DSP) built into the Remote Office 9150 unit's motherboard

What trunk interface modules do

Trunk interface modules route calls over the circuit-switched network. The number of modules you must install depends on the number of simultaneous calls you want to process in host-controlled or local-controlled mode.

Note: To determine how many trunk interface modules you need for your calling requirements, use the "Remote Office 9150 System expansion worksheet" on page 437.

What DSP application modules do

DSP application modules convert voice and fax into digital data for transport over the IP and circuit-switched networks.

Initially, the Remote Office 9150 unit ships with the ability to support up to eight simultaneous calls through a DSP that is built into the Remote Office 9150 unit's motherboard. To add support for up to 32 simultaneous calls, you must install DSP application modules. Up to three DSP application modules are supported. Each module provides up to eight more simultaneous calls.

Note: To determine how many DSP application modules you need for your calling requirements, use the "Remote Office 9150 System expansion worksheet" on page 437.

When to install trunk interface or DSP application modules

Perform the procedures in this section when you

- need to expand the Remote Office 9150 unit's voice processing capability and have ordered additional modules (up to four trunk interface modules or three DSP application modules)
- need to replace a module because it is faulty

Before you begin

Before you can install a trunk interface or DSP application module, you must remove the cover from the Remote Office 9150 unit. For instructions, see "Removing the Remote Office 9150 unit cover" on page 113.

ATTENTION

DSP application and trunk interface modules are sensitive pieces of electronic equipment and must be handled as such. Ensure that you follow the electrostatic discharge safety precautions described on page 109.

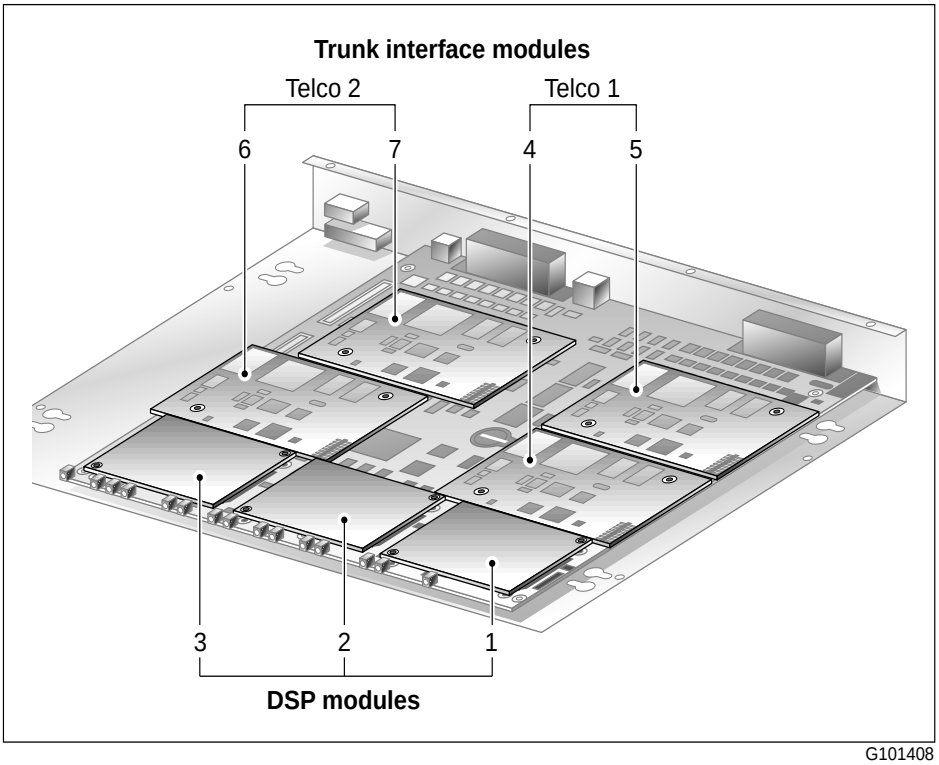
Where the modules can be installed

Each module position is labeled on the Remote Office 9150 unit circuit board as shown in the following table:

Module type	Valid module positions
DSP application module	■ MOD 1 ■ MOD 2 ■ MOD 3
Trunk interface module	Telco 1 connector (phone lines 1 through 16): ■ MOD 4 ■ MOD 5

Module type	Valid module positions
Trunk interface module (continued)	Telco 2 connector (phone lines 17 through 32): ■ MOD 6 ■ MOD 7 **Note:** Each Telco connector provides access to two ISDN BRI lines (each with two B-channels).

The following diagram shows where you can install the trunk interface and DSP application modules on the Remote Office 9150 unit circuit board:



Nortel Networks recommends that you populate each module position in sequential order. Install trunk interface modules according to the Telco 1 or Telco 2 connections used.

Note: The Remote Office 9150 unit contains a dongle socket located in the middle of the circuit board. This dongle is not being used.

To remove a trunk interface or DSP application module

Note: Perform this procedure only if you need to replace a trunk interface or DSP application module.

1. Use one hand to firmly grasp the long sides of the module that you want to remove.
2. Gently lift one side of the module up until it is free of the connectors on the Remote Office 9150 unit circuit board.
3. Lift the module up and away from the Remote Office 9150 unit circuit board, and place it to one side.

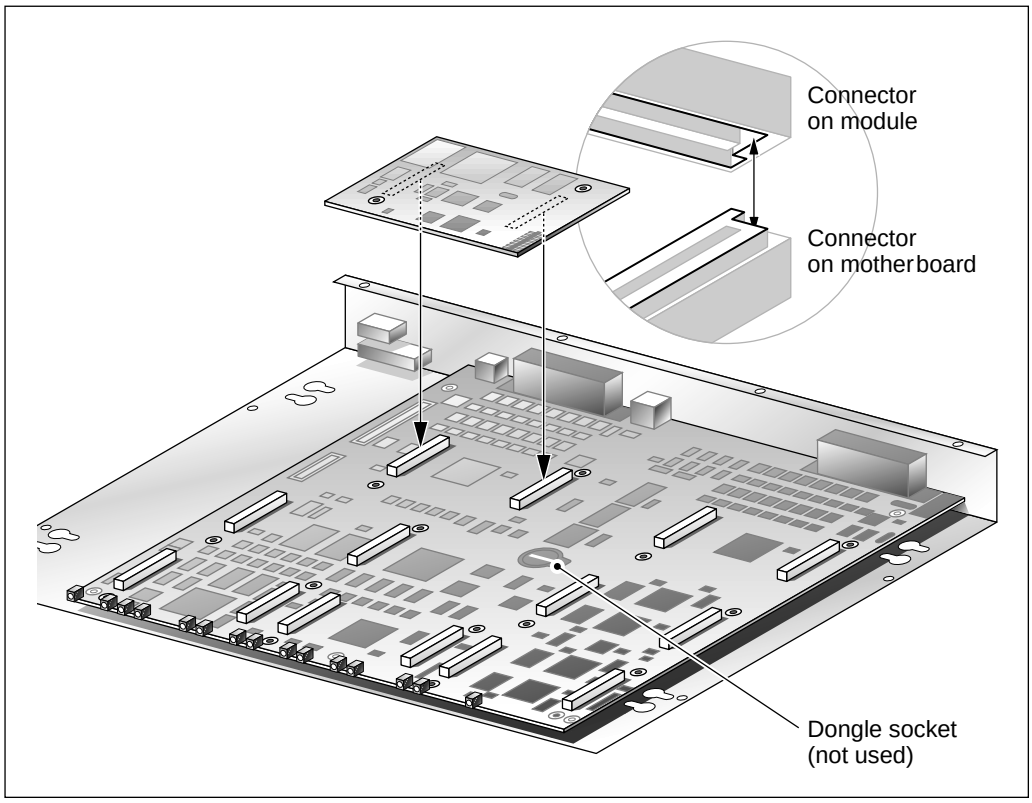
   Note: If you are replacing this module, put it inside the replacement module's protective wrapper for storage or return it to Nortel Networks for repair.

To install a trunk interface or DSP application module

1. Remove the trunk interface or DSP application module from its protective wrapper.
2. Compare the connectors on the module with the connectors in the location where you want to install the module.

   The connectors are keyed so that you can install the module in one way only. Ensure you hold the module so that the orientation of the connector keys match.

   See "Where the modules can be installed" on page 117, and the diagram on page 120.



G101404

3 Align the connectors on the module with the connectors on the Remote Office 9150 unit circuit board.

4 Use both hands to grasp the module firmly and push down until it snaps into place.

5 Visually inspect the module connectors to ensure there is no gap between the module connectors and the Remote Office 9150 motherboard connectors.

6 Ensure the module is securely installed by placing one finger beneath the module and tugging upward. The module should not move.

What's next?

After you have installed the trunk interface or DSP application modules, replace the Remote Office 9150 unit cover, and then install the unit in its chosen location. For instructions, see the following:

- "To replace the Remote Office 9150 unit cover" on page 115
- "Mounting the Remote Office 9150 unit" on page 122

Module configuration

To associate the ISDN BRI line from your ISDN service provider with a particular trunk interface module, you must configure the trunk interface modules in Configuration Manager.

If you have installed one or more modules as part of your first-time installation, complete the remaining procedures in this chapter. Then, complete configuration as required and described in "Configuring BRI trunks" on page 242.

Mounting the Remote Office 9150 unit

Introduction

The Remote Office 9150 unit can be installed

- on a desk (see below)
- on a wall (see page 124)
- in a rack (see page 126)

The Remote Office 9150 unit package contains the following hardware:

- rubber feet for installing the Remote Office 9150 unit on a desk
- brackets with screws for installing the Remote Office 9150 unit in a rack

If you want to mount the Remote Office 9150 unit on a wall, you must provide your own mounting hardware.

Choosing a suitable location

The Remote Office 9150 unit dimensions are

- 42.5 cm (17 in.) wide (without rack-mounting brackets)
- 29.4 cm (11.75 in.) deep
- 4.4 cm (1.75 in.) high

For guidelines on where to install the Remote Office 9150 unit, see “Physical environment” on page 71.

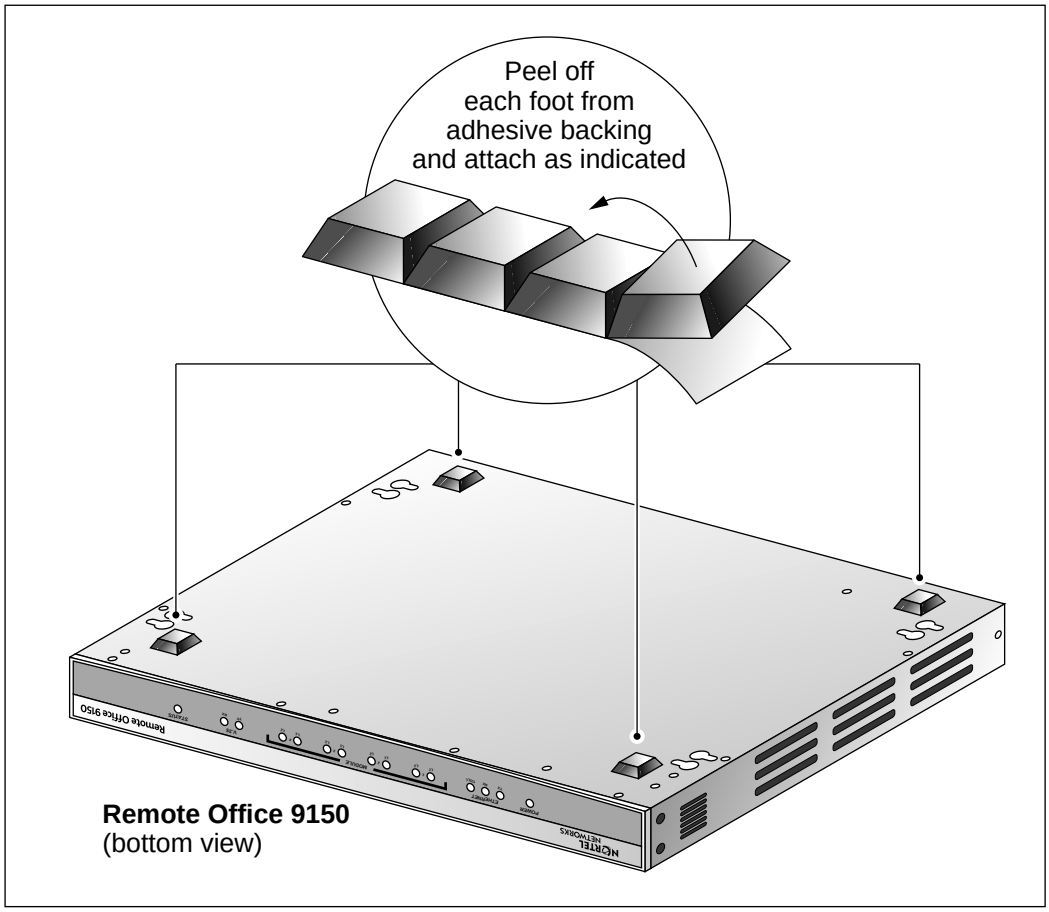
Note: It is recommended that you install the Remote Office 9150 unit in the same room where your communications equipment is installed. The Remote Office 9150 unit should be located no further than

- 1230.7 m (4000 ft) from the digital telephones
- 307.7 m (1000 ft) from the analog device

To install the Remote Office 9150 unit on a desk

1 Turn the Remote Office 9150 unit bottom side up.

2 Affix the rubber feet to the Remote Office 9150 unit as shown in the following diagram:



Remote Office 9150
(bottom view)

G101395

3 Ensure the rubber feet are securely fastened.

4 Place the Remote Office 9150 unit in the desired location.

5 Continue with “Connecting the Remote Office 9150 unit” on page 129.

To install the Remote Office 9150 unit on the wall

Do not affix the rubber feet to the bottom of the Remote Office 9150 unit. Otherwise, the unit cannot be mounted flush against the wall.

To mount the Remote Office 9150 unit on the wall, you must provide your own screws. You need suitable size screws that are long enough to ensure the Remote Office 9150 unit is securely mounted.

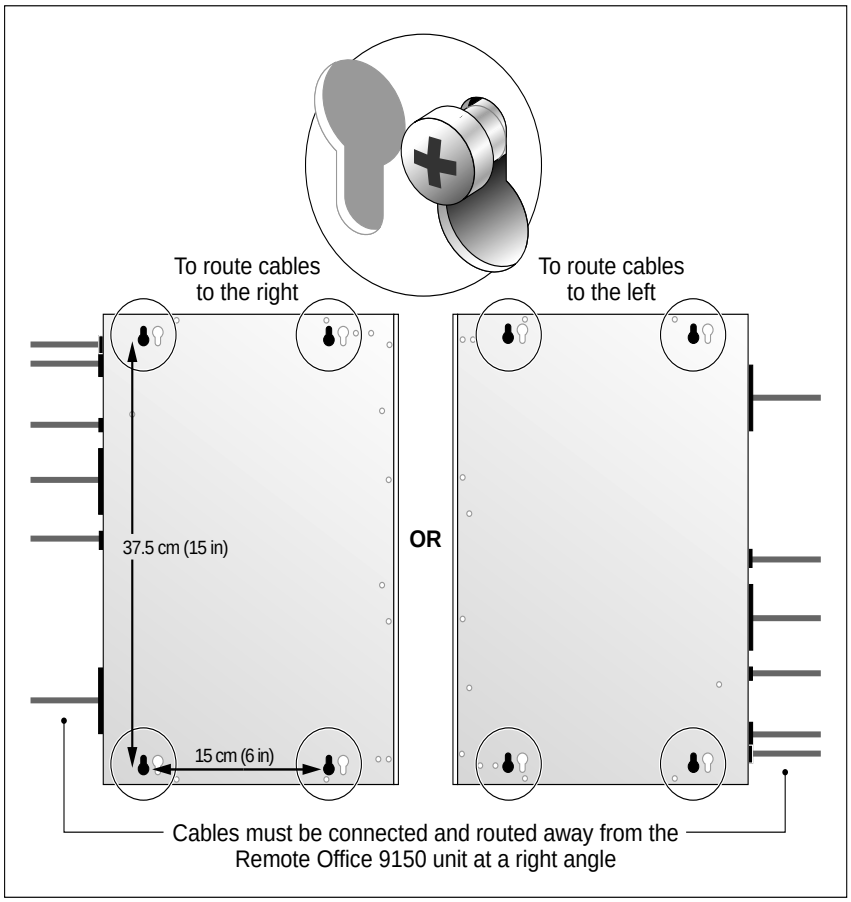
When mounting the Remote Office 9150 unit on the wall, you must use standard telephony installation practices. The unit is mounted so that

- the cables are at right angles to the unit
- the rear (connection) panel faces left or right

Ensure that

- the LEDs on the front panel can be viewed easily
- the chosen location provides enough space to accommodate the cables when they are connected to the Remote Office 9150 unit

See the diagram on page 125.



1 Choose the location on the wall where you want to mount the Remote Office 9150 unit.

2 Use the predrilled screw slots on the bottom of the Remote Office 9150 unit as a guide to measure and mark the location on the wall for each mounting screw.

The measurements between the screw slots are as follows:

- from front to back panels: 15 cm (6 in.)
- from side to side: 37.5 cm (15 in.)

Note: Two sets of screw slots are provided. Each set allows you to route the cables to the left or right when the Remote Office 9150 unit is correctly mounted. Ensure you use the same screw slot orientation for each location that you mark on the wall.

3 Mount the screws.

Note: Do not screw the screws all the way in. The heads should be screwed to about 5 mm (1/8 in.) from the wall.

4 Mount the Remote Office 9150 unit on the screws, and then gently pull it down so the screws slide into the narrow portion of the screw slots.

Do not let go yet!

5 Ensure the Remote Office 9150 unit is securely mounted.

WARNING

Risk of personal injury or equipment damage

Ensure the Remote Office 9150 unit is securely fastened to the wall. Otherwise, it can fall, be damaged, and cause injury to yourself or others.

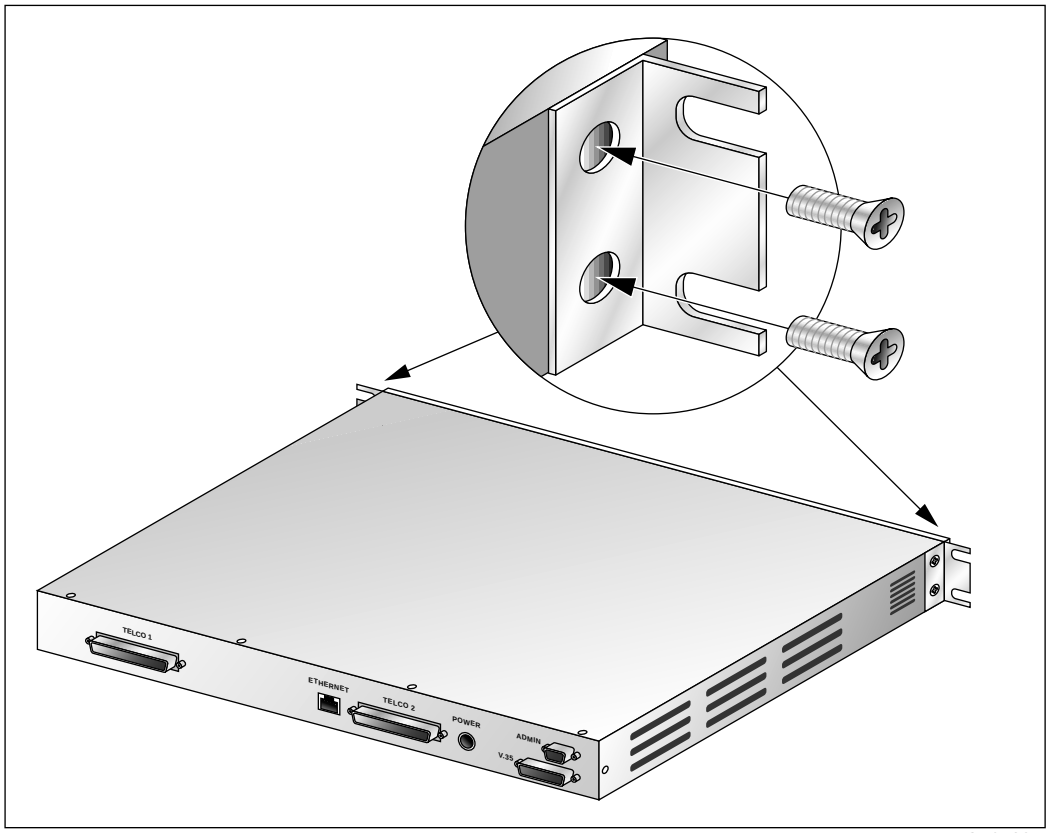
6 When you are satisfied that the Remote Office 9150 unit is securely mounted, continue with “Connecting the Remote Office 9150 unit” on page 129.

To install the Remote Office 9150 unit in a rack

The rack slot chosen for the Remote Office 9150 unit must

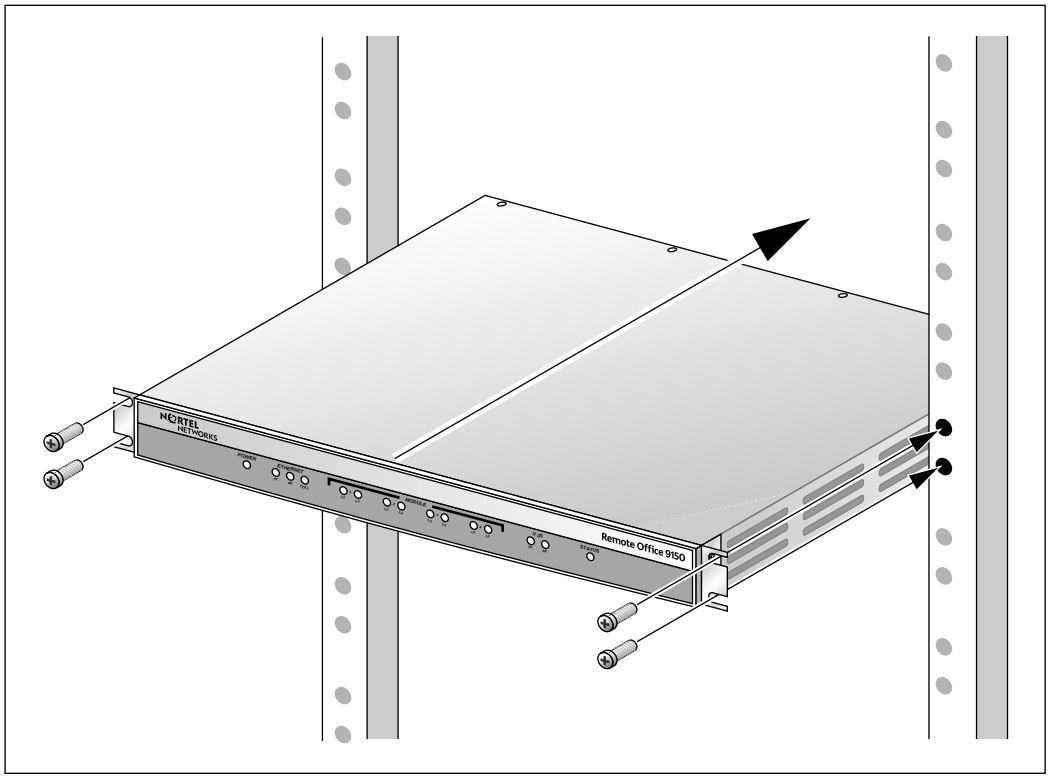
- be large enough to provide air circulation to keep the Remote Office 9150 unit cool
- allow you to securely fasten the Remote Office 9150 unit to the rack using the rack-mount brackets

1 Attach the rack-mount brackets as shown in the following illustration.



G101397

2 Slide the Remote Office 9150 unit into the rack slot.



G101398

3 Secure the Remote Office 9150 unit to the rack with nuts and bolts.

4 When you are satisfied that the Remote Office 9150 unit is securely installed, continue with “Connecting the Remote Office 9150 unit” on page 129.

What’s next?

When you have completed the installation of the Remote Office 9150 unit in its chosen location, attach the cables. For instructions, see “Connecting the Remote Office 9150 unit” on page 129.

Connecting the Remote Office 9150 unit

Introduction

When you establish the cabling connections, you are connecting the Remote Office 9150 unit to the

- power source
- telephones and ISDN BRI trunks

  Note: If you are connecting the Remote Office 9150 unit to a Meridian 1 in-building cross-connect system, you need a QCBIX1A BIX block.
- Ethernet network
- administration PC

Cables you must provide

Ensure that you have obtained the telephone and Ethernet cables for your network. These cables are not supplied in the Remote Office 9150 unit package.

The cables must meet the following requirements:

- telephone cable: One end of the cable must provide a male 50-pin connector. (This end connects to the Remote Office 9150 unit.)

  Ensure the other end of the cable matches the connectors needed to connect to the telephones or trunks. (For example, if you are using a BIX block to establish the telephone connections, the wires inside must be exposed.)

  Notes:

  - Two telephone cables are required, depending on how many telephones and trunks are installed. (Each telephone cable provides support for up to 16 digital telephones, and two ISDN BRI lines providing two B-channels each. The Telco 1 cable also provides support for one analog station such as a fax machine.)
  - Digital telephones should be located no further than 1230.7 meters (4000 feet) from the Remote Office 9150 unit.
  - The analog device should be located no further than 307.7 meters (1000 feet) from the Remote Office 9150 unit.

- Ethernet cable

  If you are connecting the Remote Office 9150 unit to a hub, you need a standard CAT5 unshielded twisted-pair (UTP) straight-through Ethernet cable. The cable should be no longer than 100 meters (325 feet) in length.

Connector and pin-out reference

The following table identifies where to find the pin-out table for each connector:

Connector	Connection type	For the pin-out table, see
TELCO 1	25 TIP and RING pairs	page 476.
TELCO 2	25 TIP and RING pairs	page 478.
ETHERNET	RJ-45	page 480.
ADMIN	DB-9	page 481.
Power	DIN	page 482.

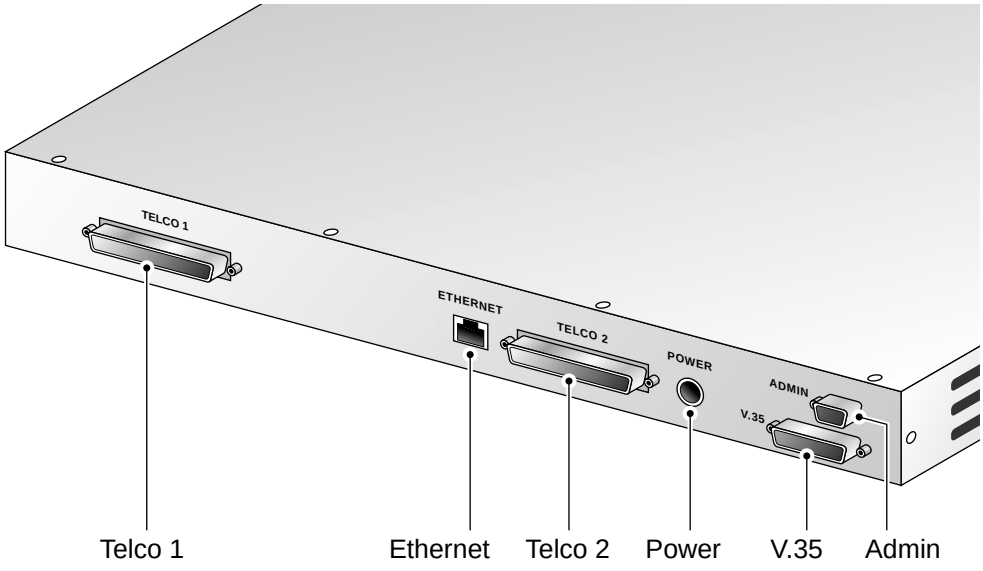
More information

The following documents describe how to establish telephone and trunk connections using the Meridian 1 BIX in-building cross-connect system:

- *Meridian 1 Installation planning* (NTP 553-3001-120)
- *Telephone and attendant console installation* (NTP 553-3001-215)
- *BIX* In-Building Cross-Connect System Material Installation and Servicing (Wall-Mounted System)* (NTP 631-4511-200)

Remote Office 9150 unit connection panel

The following diagram shows the connectors on the back panel of the Remote Office 9150 unit.

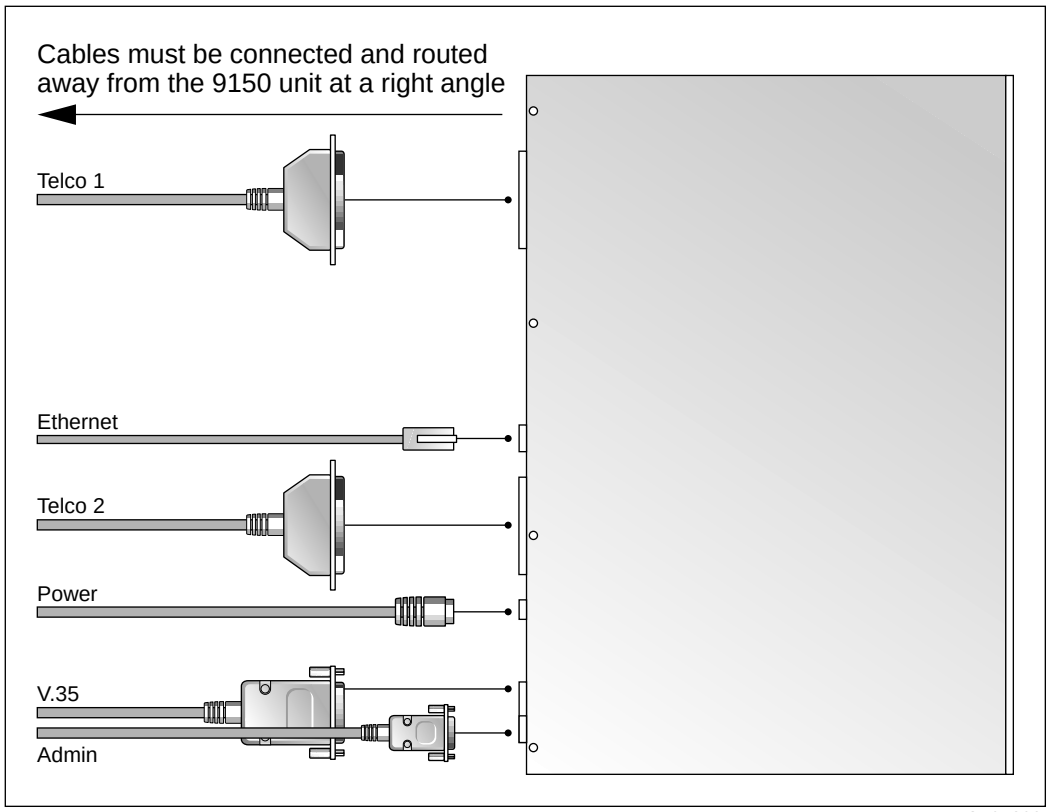


Note: The V.35 connector is for future use.

G101403

Wall-mount cable attachment

If you mounted the Remote Office 9150 unit on the wall, the following diagram shows cable attachment.



G101399

To connect the Remote Office 9150 unit to the network

WARNING

Risk of electric shock or damage to equipment

To reduce the risk of electric shock to yourself or damage to the Remote Office 9150 unit, ensure that the power source to the unit is turned off until the Telco 1 and Telco 2 connections have been completed.

1. Connect the male 50-pin connector of the telephone cable to the TELCO 1 connector on the Remote Office 9150 unit.

   Secure the cable connection by snapping the wire tabs into place or by inserting screws.

2. Refer to the pin-out table in “TELCO 1 connector pin-out table” on page 476 (in Appendix D) for establishing the connections to the telephones and trunks.

3. If you want to route calls over the IP network, or administer the Remote Office 9150 unit from another location on the IP network, connect the Remote Office 9150 unit to the Ethernet network by doing the following:

   a. Connect one end of the RJ-45 Ethernet cable to the ETHERNET connector on the Remote Office 9150 unit.

   b. Connect the other end to an Ethernet hub.

4. Connect the male 50-pin connector of the other telephone cable to the TELCO 2 connector on the Remote Office 9150 unit.

   Secure the cable connection by snapping the wire tabs into place or by inserting screws.

5. Refer to the pin-out table in “TELCO 2 connector pin-out table” on page 478 (in Appendix D) to establish the connections to the telephones and trunks.

6 Connect the ADMIN connector on the Remote Office 9150 unit to the administration PC as follows:

a. Connect the male 9-pin connector of the supplied RS-232 serial cable to the ADMIN connector on the Remote Office 9150 unit.

Note: You may need to provide an RS-232 adapter if the available RS-232 port on your PC does not match the connector on the serial cable.

b. Connect the other end to an available COM port on the PC.

7 Connect the Remote Office 9150 unit to the power source as follows:

a. Connect the four-pin plug on the power transformer to the POWER connector on the Remote Office 9150 unit.

Note: Ensure the arrow on the four-pin plug faces up.

b. Connect the AC cord to the AC power receptacle on the power transformer.

c. Plug the AC cord into a 110 V or 220 V uninterruptible power source (UPS) or wall outlet.

8 Proceed with “Powering up the Remote Office 9150 unit” on page 135.

Powering up the Remote Office 9150 unit

Introduction

As soon as you connect the Remote Office 9150 unit to the power source, the unit begins to power up.

What happens during power-up

During power up, the following events occur:

- The Remote Office 9150 unit performs a self-test that verifies all critical functionality.
- An LED test sequence is performed.

Power-up self-test

During power-up, the Remote Office 9150 unit performs a self-test that verifies all critical functionality, including

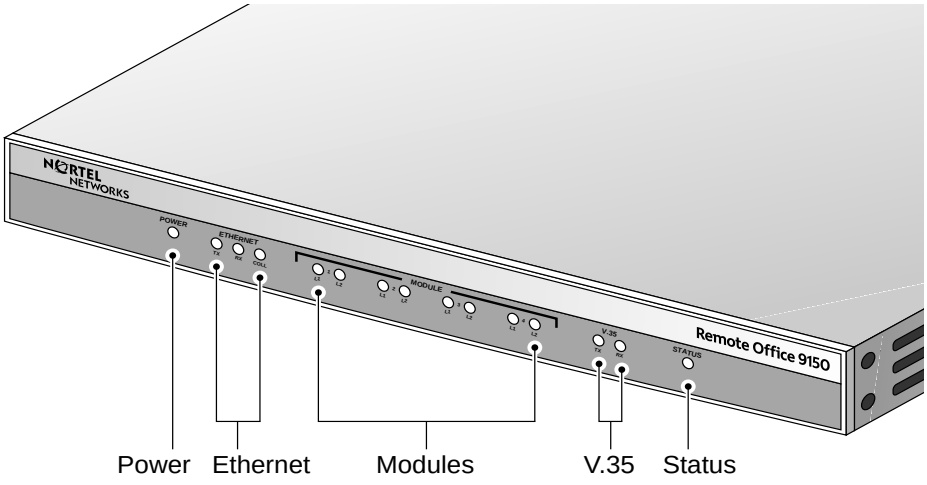
- RAM memory test
- EPROM checksum validation
- flash checksum validation
- DSP health
- interface loopbacks

The power-up cycle also automatically detects if one or more DSP application or trunk interface modules have been installed. If trunk interface modules have been installed, you can configure them in Configuration Manager.

The power-up cycle takes about 60 seconds to complete.

LED test sequence

The following diagram shows the LEDs on the front panel.



Note: The V.35 LEDs are for future use.

G101402

During the power-up cycle, the LEDs behave as follows:

1. All LEDs light for about 15 seconds.
2. The Module LEDs light individually in sequence (1 through 8).
3. All LEDs light.
4. All LEDs except the Status LED go out. The Status LED remains lit.

Note: Steps 2 through 4 take about 4 to 5 seconds.

After this point, the Remote Office 9150 unit is functional.

Notes:

- The ETHERNET TX and RX and module (ISDN BRI) LEDs flash only when transmit and receive activity is present on those interfaces.
- The ETHERNET COLL LED flashes when a data collision occurs on the line.

What's next?

If the power-up cycle completes successfully (indicated by a lit Status LED), your hardware installation is successful. Continue with "Installing the software" on page 138.

If the power-up cycle was not successful (indicated by the Status LED going out), contact your Nortel Networks distributor. There is a possible hardware problem.

Installing the software

Introduction

You use the Configuration Manager software to configure and administer the Remote Office 9150 unit. This software is located on the CD-ROM provided in the package. You must install the software on the administration PC.

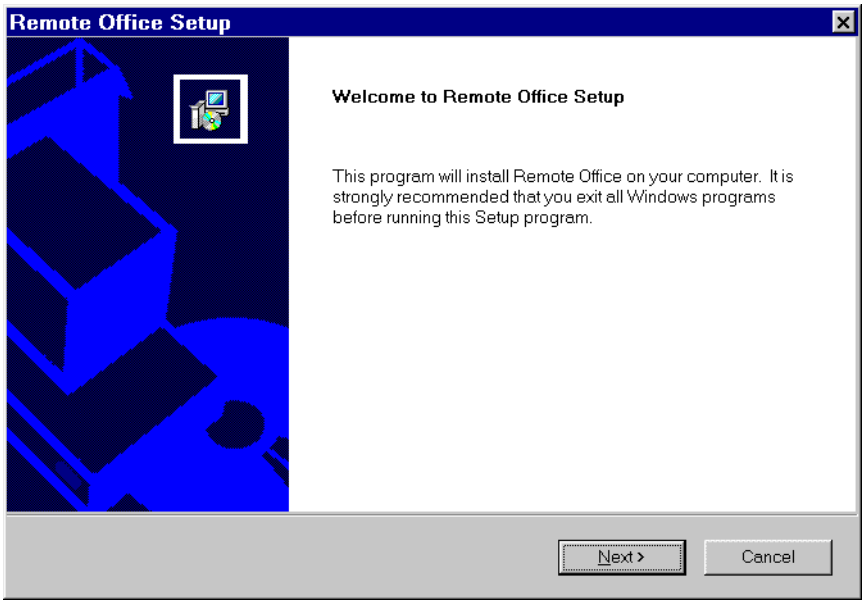
To install the software

1 Insert the CD-ROM in the applicable drive on your PC.

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, navigate to the software directory, and then locate and double-click setup.exe.

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

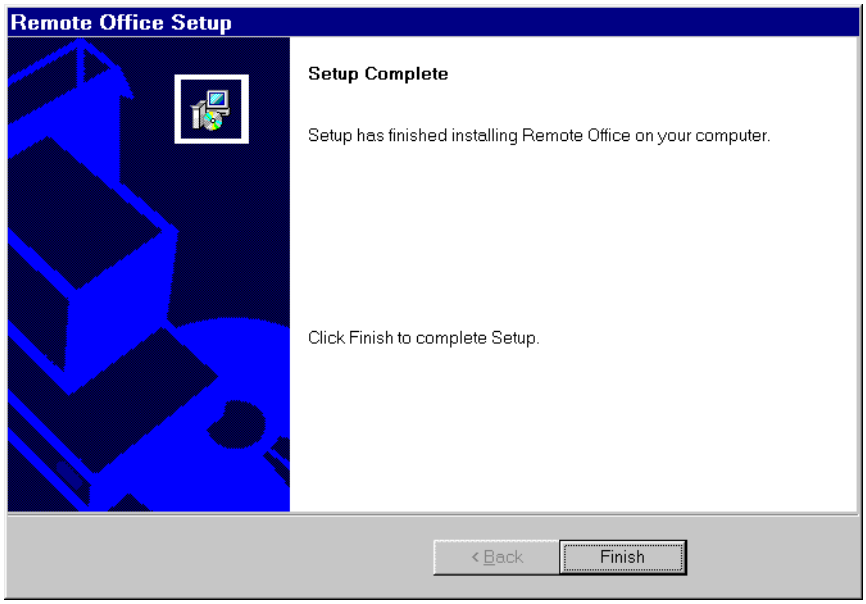


3 Click Next, and then follow the screen prompts.

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.



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

5 Click Finish.

Result: The InstallShield closes.

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 141.

Note: DLL files installed by the Configuration Manager InstallShield should be left 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 Remote Office 9150 unit and the MIG RLC at the host site. The Configuration Wizard does not provide all the configuration settings that are available in Configuration Manager. By using the Configuration Wizard, the Remote Office 9150 unit can be up and running within 10 minutes.

You can use the Configuration Wizard in offline mode or while connected and logged on to the Remote Office 9150 unit (online mode).

What you can configure with the Configuration Wizard

The Configuration Wizard allows you to configure the following:

- the Remote Office 9150 unit'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, you can use the sample information provided in the procedure on page 146.
- for Voice over IP capability: the IP address for the MIG RLC at the host site
- for circuit-switched network capability:
  - the telephone number of the MIG RLC at the host site
  - information provided by your ISDN service provider for each ISDN BRI trunk interface module (telephone numbers, SPIDs, and switch type)

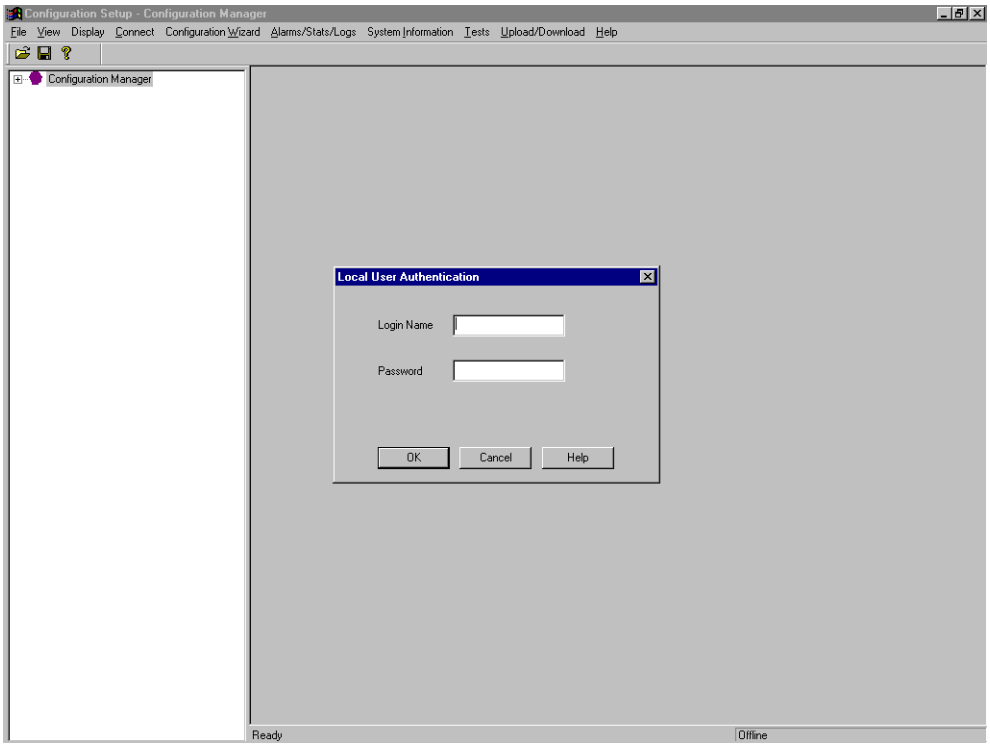
Ensure you have this information ready before you begin.

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



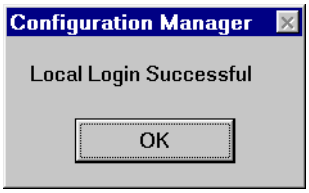
2 Type **admin** into the Login Name box.

3 Type **root** into 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 logon status dialog box disappears.

6 Do one of the following:

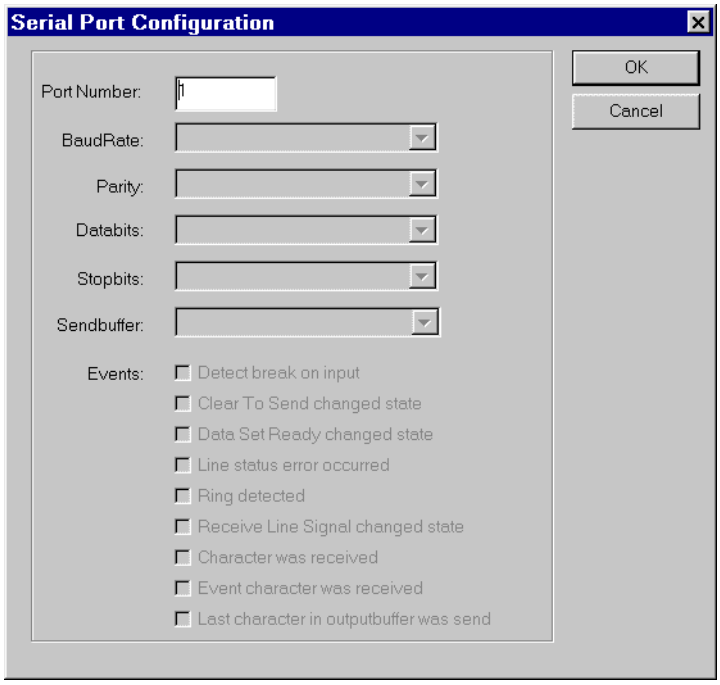
IF you want to perform an	THEN
offline configuration	do the following: **a** Choose View → Device Type → 9150. **b** Continue with "To perform configuration with the Configuration Wizard" on page 146.
online configuration	continue with "To establish a serial connection" below.

To establish a serial connection

Note: If you want to perform an offline configuration, ignore this procedure. Go to "To perform configuration with the Configuration Wizard" on page 146.

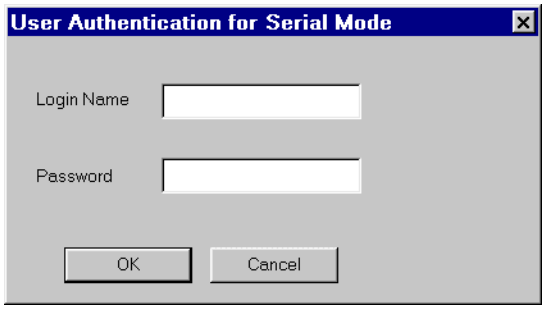
1 From the menu, choose Connect → Login board → Serial.

Result: The Serial Port Configuration dialog box appears.



2 Enter the COM port to which the Remote Office 9150 unit is connected, and then click OK.

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



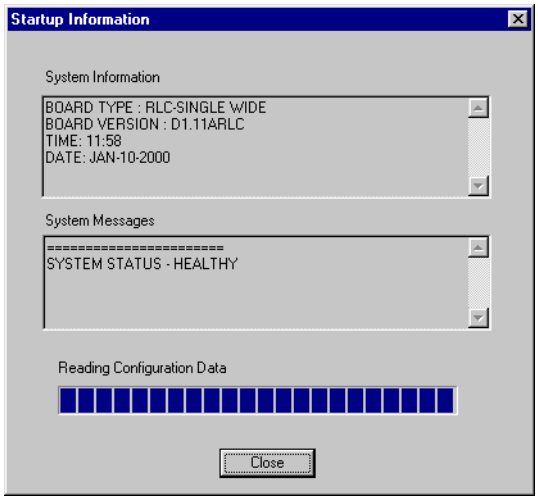
3 Type **guest** for the logon name.

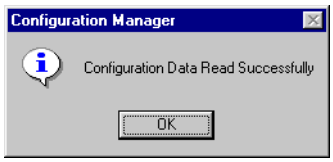
4 Type **guest123** for the password.

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

5 Click OK.

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

IF the logon attempt	THEN
failed	the following message appears: `SERIAL CONNECTION FAILED` Check the serial connection and ensure it is good. Then, go back to step 1.
succeeded	the User Logged In dialog box appears. Click OK. **Result:** The following dialog box appears:  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:  Click OK.

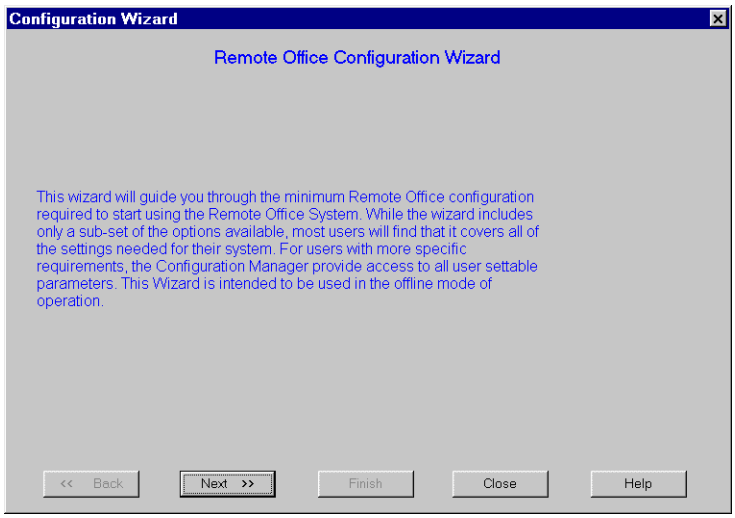
6 Continue with “To perform configuration with the Configuration Wizard.”

To perform configuration with the Configuration Wizard

Note: The screen examples in this procedure use information from the sample network diagram in “Example of a network” on page 462.

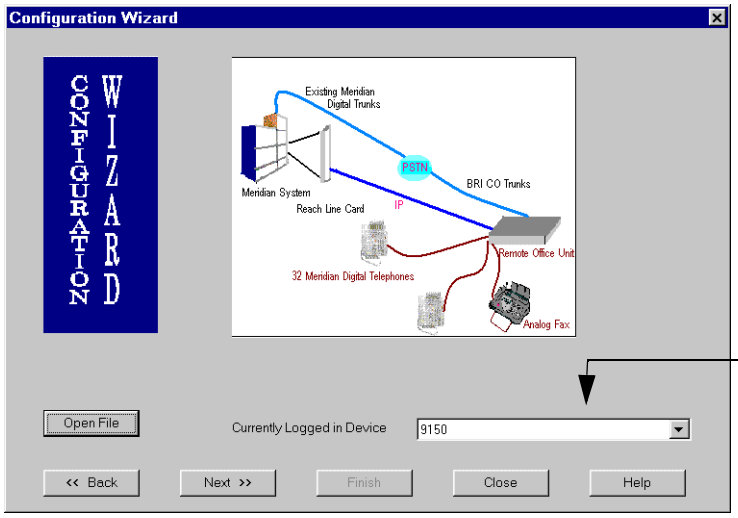
1 Choose Configuration Wizard from the menu.

Result: The following screen appears:



2 After reviewing the message, click Next.

Result: The following screen appears:



3 Verify that the Currently Logged in Device box shows 9150, then click Next.

If it does not show 9150, then select 9150 from the list box.

Result: The Local Unit Configuration screen appears.

Note: A completed example is shown on page 148.

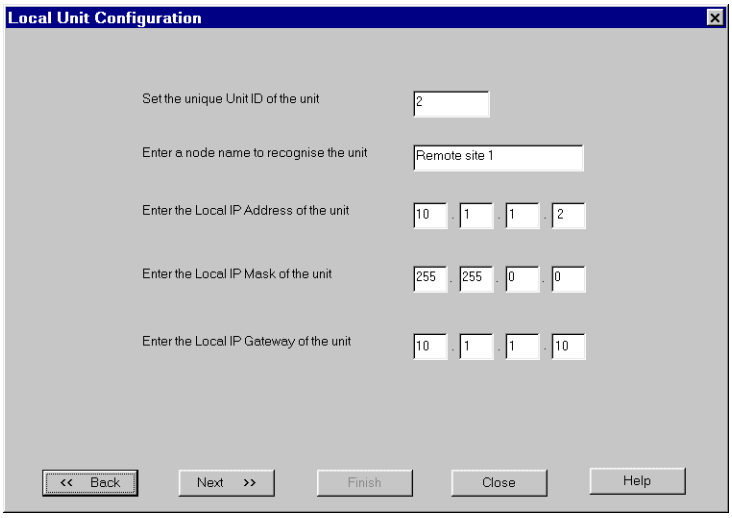
4 Complete the fields on this screen as described in the following table:

Field	Description
Set the unique Unit ID of the unit	Enter the number from 1–255 that uniquely identifies the Remote Office 9150 unit you are configuring for a particular MIG RLC. **Note:** Each unit connected to a MIG RLC must be given a unique unit ID. This implies that Remote Office 9150 units that connect to different MIG RLCs in the network can have the same unit ID.
Enter a node name to recognize the unit	Enter a name that uniquely identifies the Remote Office 9150 unit you are configuring.

Field	Description
Enter the local IP Address of the unit	Enter the IP address assigned to the Remote Office 9150 unit. **Note:** If you do not have a valid IP address, type the sample IP address: **10.1.1.2**.
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 Remote Office 9150 unit and the network. **Note:** If there is no router between the Remote Office 9150 unit and the network, then the administration PC acts as the gateway. Type **10.1.1.10**. ■ as the IP address on the administration PC ■ as the gateway on the Remote Office 9150 unit

The following is a completed example:

The IP information allows you to administer the Remote Office 9150 unit from any location on the network.



5 Click Next.

Result: The Set the Configuration for the Remote Unit screen appears.

Note: A completed example is shown on page 150.

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

Field	Description
Set the Unit ID of the RLC to connect to	Enter the MIG RLC's unit ID.
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 of the MIG RLC to which this Remote Office 9150 unit is connected. ■ Click No if the IP network will not be used. The IP Address boxes are dimmed.
Wish to Enable PSTN Connection to Remote	■ Accept Yes if the circuit-switched network will be used to route calls. Then, enter the telephone number that must be dialed to connect to the MIG RLC. 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 Number box is dimmed.

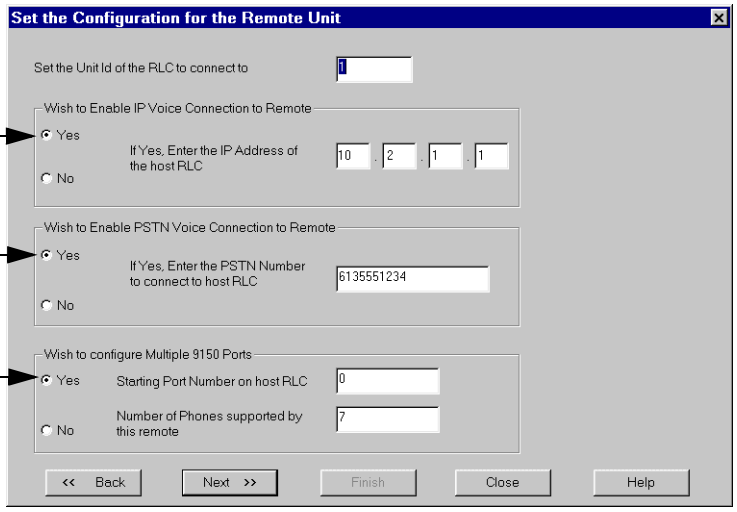
Field	Description
Wish to configure Multiple 9150 Ports	■ Click Yes if you want to assign Remote Office 9150 ports to digital telephones now. Then, do the following: ■ Enter the first MIG RLC port number to assign. **Note:** Nortel Networks recommends that ports be configured so that the MIG RLC port number matches the Remote Office 9150 unit's port number. ■ Enter the number of telephones connected to the Remote Office 9150 unit. ■ Click No if you want to complete port assignment at a later time with Configuration Manager.

The following is a completed example:

Click Yes to allow voice calls over IP, then enter the MIG RLC's IP address.

Click Yes to allow voice calls over the circuit-switched network, then enter the MIG RLC's phone number.

Click Yes to automatically assign Remote Office 9150 unit ports to MIG RLC ports, then enter the information as described previously.



7 Click Next.

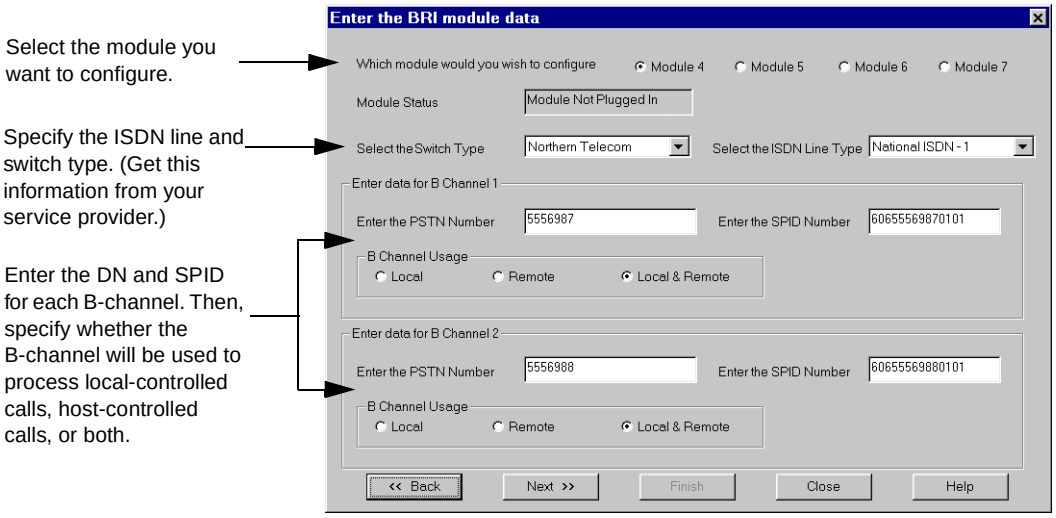
Result: The Enter the BRI module data screen appears.

Note: A completed example is shown on page 152.

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

Field	Description
Which module would you wish to configure	Click the number identifying the trunk interface module that you are configuring. The number you select must match the position where the module has been installed in the Remote Office 9150 unit.
Module Status	This box identifies if a module has been physically installed on the Remote Office 9150 unit.
Select the Switch Type	Select the type of switch used by your ISDN service provider.
Select the ISDN Line Type	Select the ISDN variant used in your country.
Enter the PSTN Number (B channel 1 and B channel 2)	Enter the telephone number provided by your ISDN service provider for this B-channel.
Enter the SPID Number (B channel 1 and B channel 2)	Enter the Service Profile Identifier (SPID) provided by your ISDN service provider for this B-channel.
B Channel Usage (B channel 1 and B channel 2)	Select one of the following connection types: ■ Local: This trunk is used for local PSTN calls only. ■ Remote: This trunk is used only for calls to and from the host PBX. ■ Local & Remote: This trunk can route both types of calls.

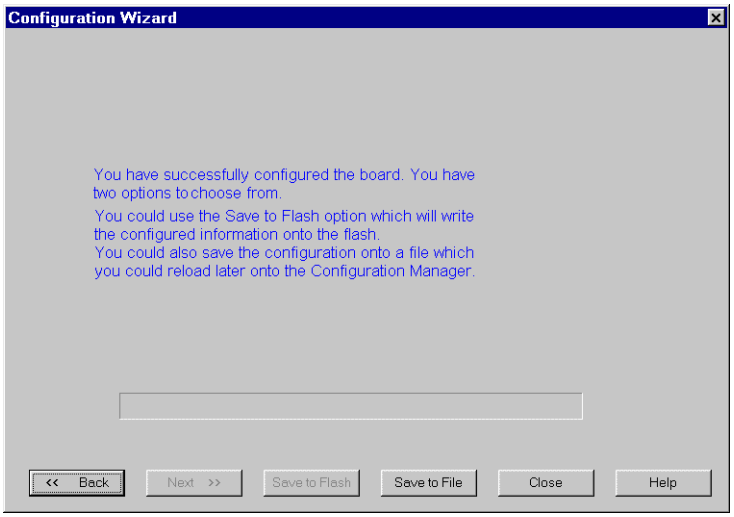
The following is a completed example.



9 Repeat step 8 for each ISDN BRI module you want to configure.

10 Click Next.

Result: The following screen appears:



11 Do 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). **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 147. The information in this file can be opened in Configuration Manager, and then sent to and saved in the Remote Office 9150 unit's flash memory at another time. For instructions, refer to "Working with configuration files" on page 183.
online configuration	**1** Click Save to Flash. **Result:** The information entered is written to the flash memory of the Remote Office 9150 unit 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. **2** Restart the Remote Office 9150 unit.

What's next?

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

- Test the network connections. For instructions, see "Testing the network connections" on page 155.
- Perform additional configuration, if needed. For instructions, see Chapter 5, "Configuring the Remote Office 9150 unit."

Testing the network connections

Introduction

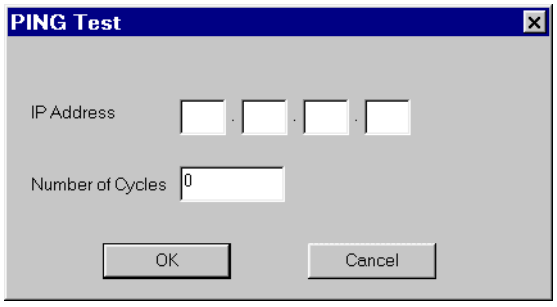
After you have installed the hardware and performed initial configuration, verify that network connectivity is present by performing the tests described in this section.

To verify IP network connectivity using PING

To test the Ethernet connection between the administration PC and the Remote Office 9150 unit, you can use PING. To do this test, the Remote Office 9150 unit and the administration PC must be physically connected to the IP network.

1 From the menu in Configuration Manager, choose Tests → Ping.

Result: The PING Test dialog box appears.



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

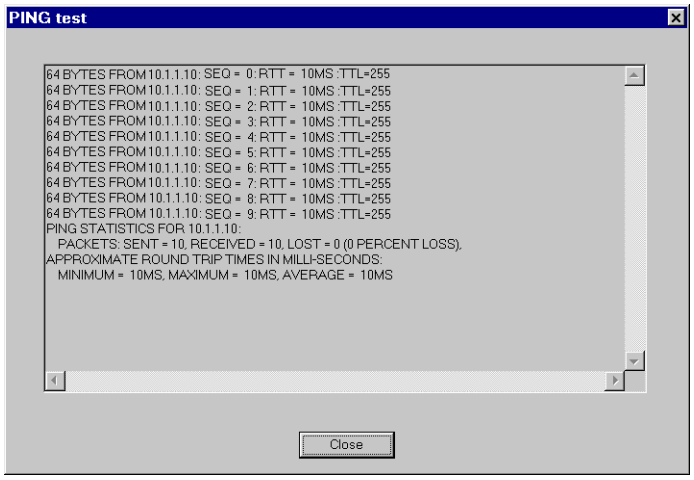
3 In the Number of Cycles box, enter the number of times you want to ping the unit.

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

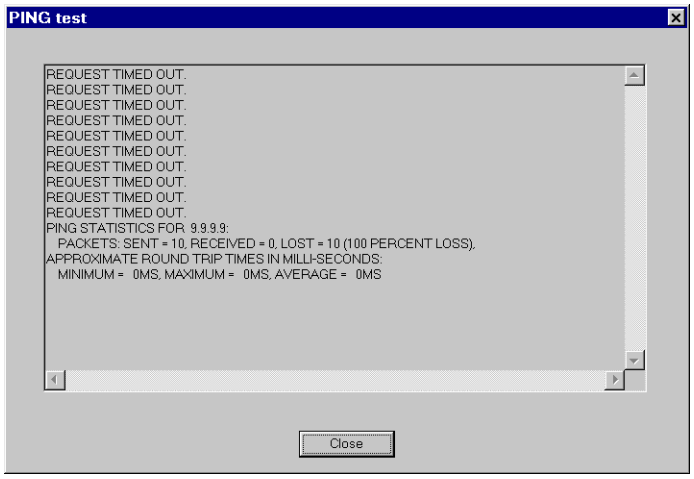
4 Click OK.

Result: The PING test results screen appears, showing the ping results.

The following is an example of a successful ping:



The following is an example of an unsuccessful ping:



5 Click Close.

Result: The Ping test screen closes.

What to do if the ping did not work

1 Use Configuration Manager to ensure you have entered the IP address, subnet mask, and default gateway correctly.

Note: For instructions, see “To enter the IP addresses” on page 228.

2 Ping the gateway to see if it responds.

3 If the ping still does not work, contact your data network administrator.

To verify the telephone network connectivity

1 Look at the digital telephone display.

Does it display the correct time and date? If yes, then the connection paths between the digital telephone, Remote Office 9150 unit, and the MIG RLC are working.

2 Lift the telephone handset, or press the host call appearance key to go off hook.

Did you receive a dial tone? If yes, then the connection path between the Remote Office 9150 unit and the MIG RLC is working.

3 Initiate an outgoing call through the host PBX.

Did the call proceed as expected? If yes, then the connection path between the Remote Office 9150 unit and the MIG RLC is working.

4 Press the local call appearance key to go off hook.

Did you receive a dial tone? If yes, then the connection path between the Remote Office 9150 unit and the digital telephone is working.

5 Initiate an outgoing call through the PSTN.

Did the call proceed as expected? If yes, then the ISDN BRI lines to the PSTN are working.

What to do if the telephone connection tests do not work

1 Ensure the Remote Office 9150 unit completed its power-up cycle successfully. If it did, the Status LED remains lit.

2 Verify the connections between the telephone network and the Remote Office 9150 unit.

3 Ensure that the placement of ISDN BRI modules within the Remote Office 9150 unit correspond with the Telco 1 and Telco 2 cable connections.

Note: Refer to the Telco 1 and Telco 2 cable pin-out tables in Appendix D, “Connection pin-out tables.”

4 Use Configuration Manager to verify that the following configuration is correct on the Remote Office 9150 unit, as appropriate:

- IP addresses (Remote Office 9150 unit, subnet mask, and default gateway, as well as the MIG RLC’s IP address, if the IP network is being used to route calls)
- the telephone number used to establish connections to the MIG RLC, if the circuit-switched network is being used to route calls
- the security IDs of both the Remote Office 9150 unit and the MIG RLC, if a security ID is required to authenticate connection attempts
- DNs and SPIDs assigned to the ISDN BRI modules installed in the Remote Office 9150 unit
- station configuration, to ensure that the telephone you are using has the calling capabilities needed to complete the tests (that is, verify that the station is correctly configured as local only, remote only, or both local and remote)

Note: For instructions on using Configuration Manager, see Chapter 5, “Configuring the Remote Office 9150 unit.”

5 Work with the administrator at the host PBX site to ensure that

- the MIG RLC is enabled and working in its PBX slot (restart the MIG RLC, if necessary)
- the configuration of the IP address, telephone number, and security ID on the MIG RLC port are correct (if these items are used)

6 Verify that both the telecom and data networks are routing voice calls as expected (that is, calls are not being blocked in any way).

What to do if nothing works

If you cannot get the system to work, contact your Nortel Networks distributor for assistance.

What's next?

Once you have confirmed that the Remote Office 9150 unit can be recognized on the network, you can fine-tune the configuration. Nortel Networks recommends that you also change the passwords used for logging on to the Configuration Manager and the Remote Office 9150 unit.

For	See
a description of Configuration Manager	Chapter 4, "Configuration Manager overview."
instructions on how to modify the configuration	Chapter 5, "Configuring the Remote Office 9150 unit."
instructions on how to change passwords	"Changing the administration password" on page 294.

Chapter 4

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, you can display the current configuration by clicking Retrieve. 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 183 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 189.

Starting Configuration Manager

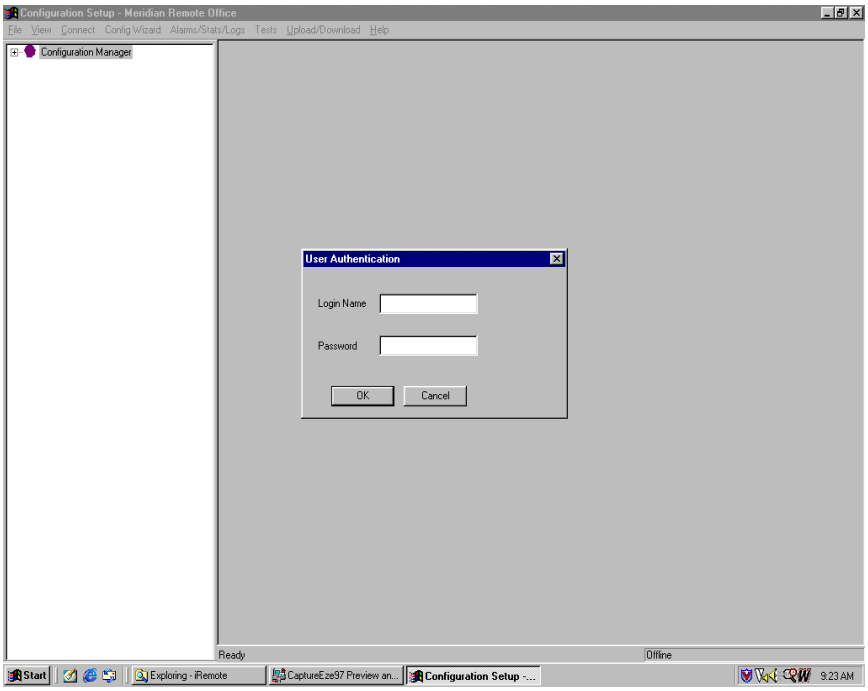
Introduction

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.

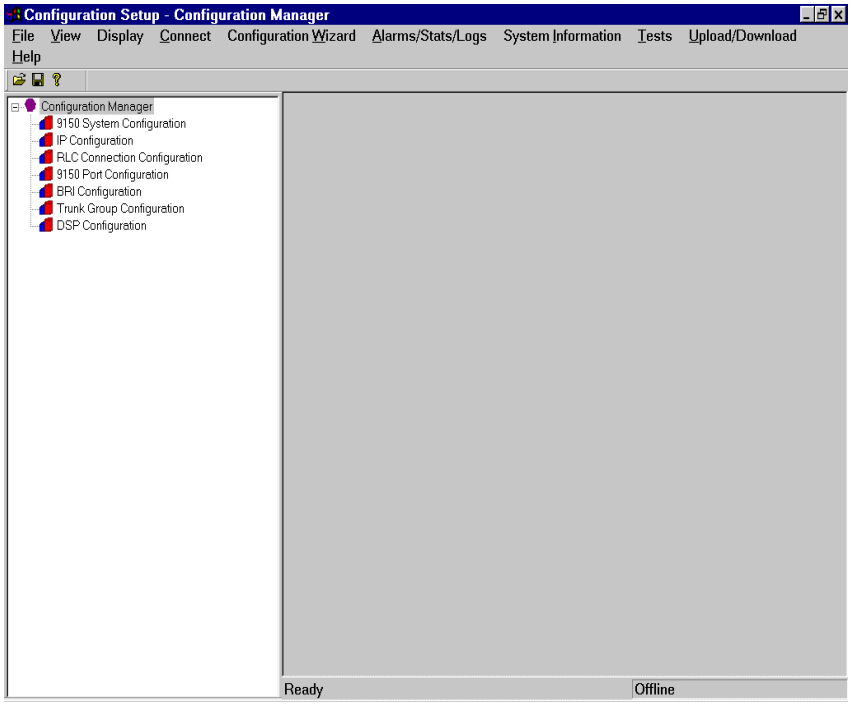
Result: The Login Name dialog box disappears.

6 Proceed as follows:

To perform an	See
online configuration	“Logging on to a unit” on page 189.
offline configuration	“Selecting the device type for offline configuration” on page 187.

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 166.


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.

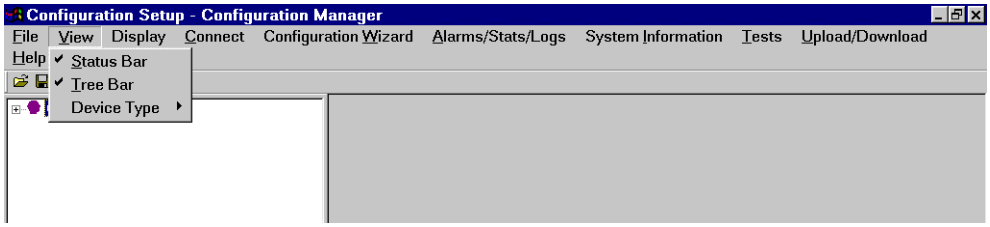
- The menu across the top of the screen lists various administrative tasks you can perform. These tasks are common to all Remote Office units.
- The pane on the left lists the property sheets you can work with. In this guide, the left pane is called the *system tree*.
- The pane on the right displays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

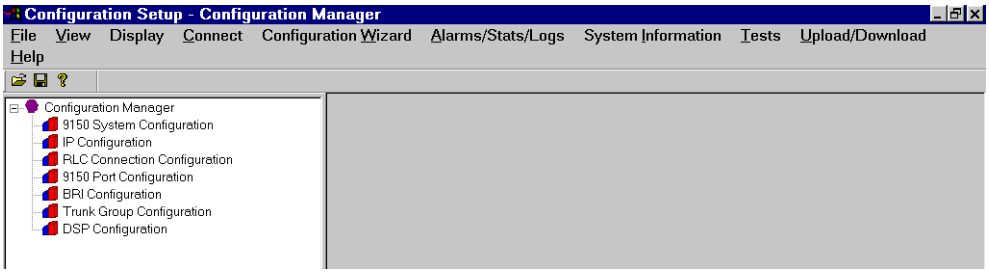
To simplify the instructions for selecting options from the menu, this guide abbreviates the selection path. For example, if a procedure requires you to choose Over IP from the Remote Connectivity menu, which is under the Tests menu, this guide uses the following style:

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:



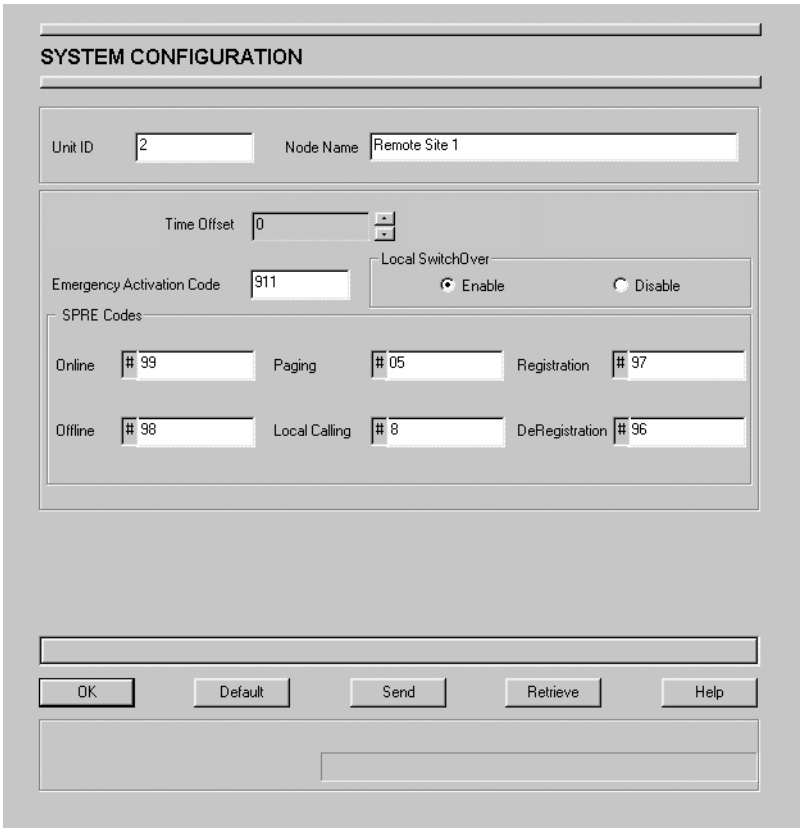
You can hide the system tree. To do this, choose View → Tree Bar. The screen redisplays, showing only the property sheet pane.

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 187.

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



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 187.
online configuration	connect to, and then log on to the Remote Office 9150 unit as described in "Logging on to a unit" on page 189.

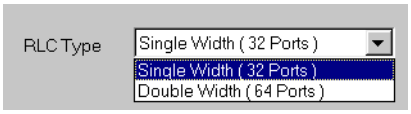
2 Navigate to the IP Configuration screen as follows:

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.



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.

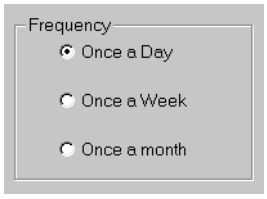
Check boxes

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).

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.



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.

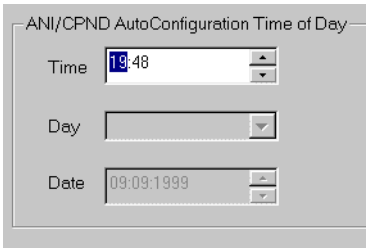
- Other fields are reenabled (no longer appear dimmed).
- One or more values on the property sheet are replaced with values that are specific to the option you selected.

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:

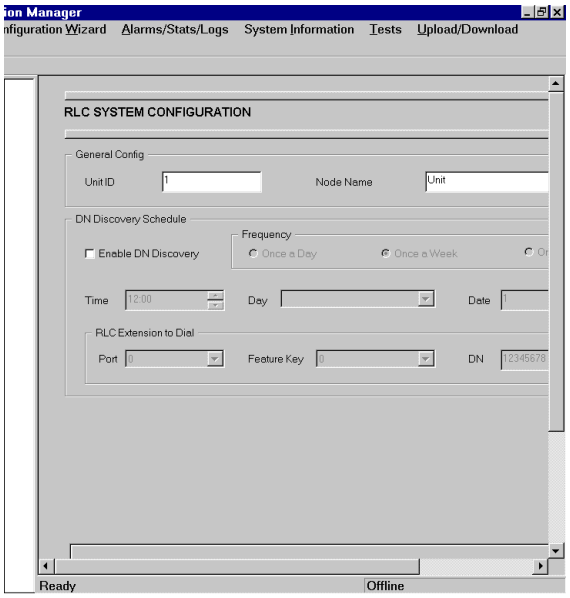


Scroll bars

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.



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 179.

- 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 180.

- Retrieve

  Retrieve downloads the unit's configuration from flash memory and displays it in Configuration Manager on your PC. For more details, see "Retrieve" on page 180.

- 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 175.

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.

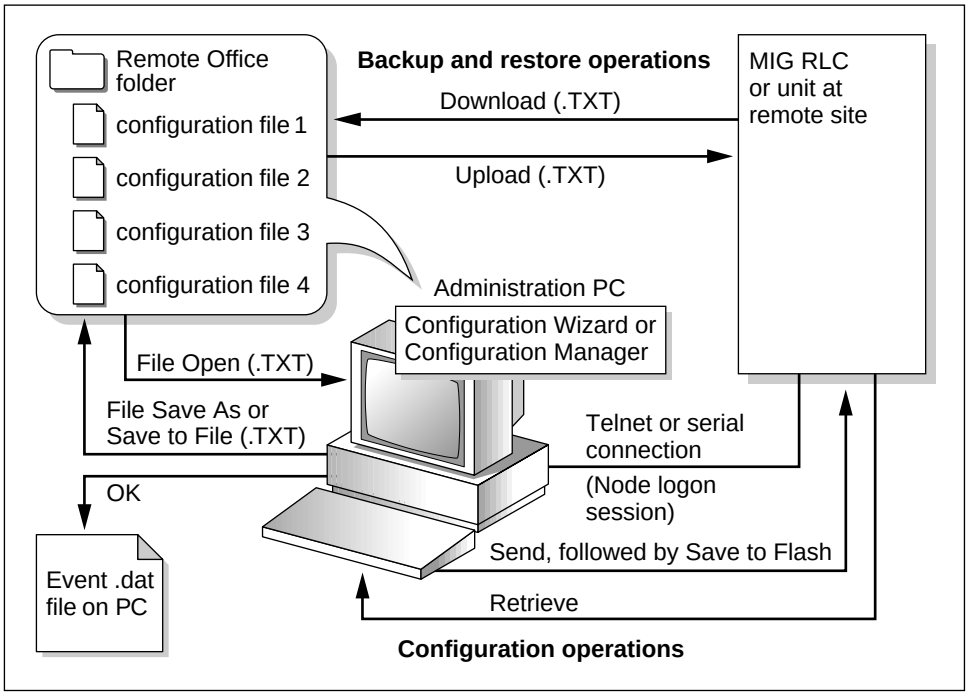
Configuration files description

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 183 ■ "Performing backups and restores" on page 299. **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 335.

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 177. 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 180. **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 the current 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 a Save to Flash from the Upload/ Download Menu 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 a Save to Flash from the Upload/ Download Menu 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 198.

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 184)
- open a configuration file in Configuration Manager (see page 185)
- perform a configuration upload (see page 186)
- perform a configuration download (see page 186)

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.
one of the following: ■ Send ■ Send All ■ Retrieve ■ Upload Configuration ■ Download Configuration	connected and logged on to a unit.

To create a configuration file on the PC

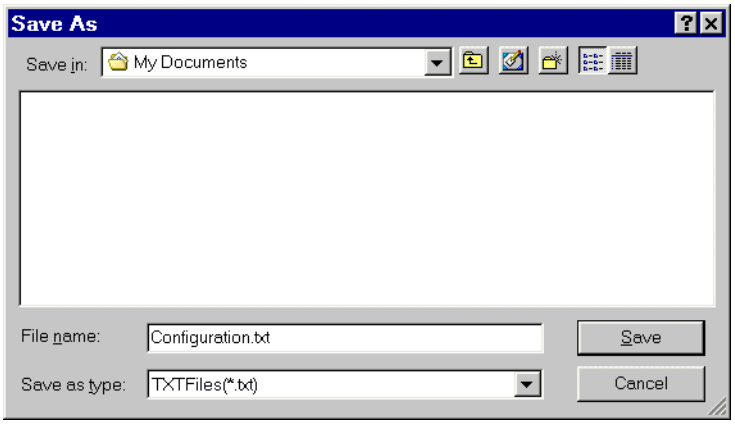
1 Start Configuration Manager.

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.



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.

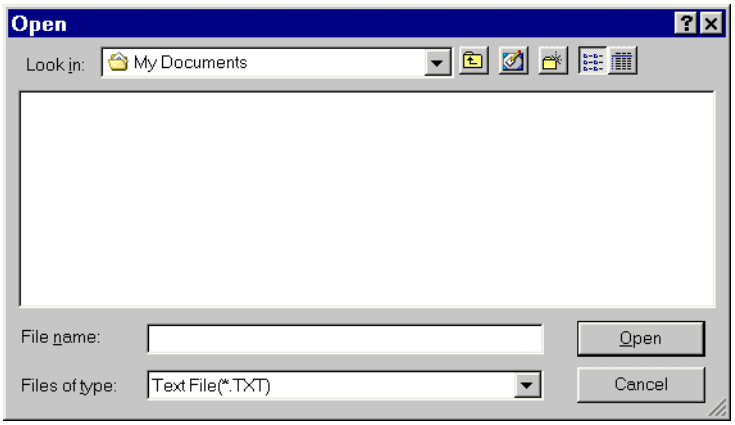
To open a configuration file

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 303.

To download a configuration from a unit

For instructions, see “Creating a backup configuration file” on page 301.

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

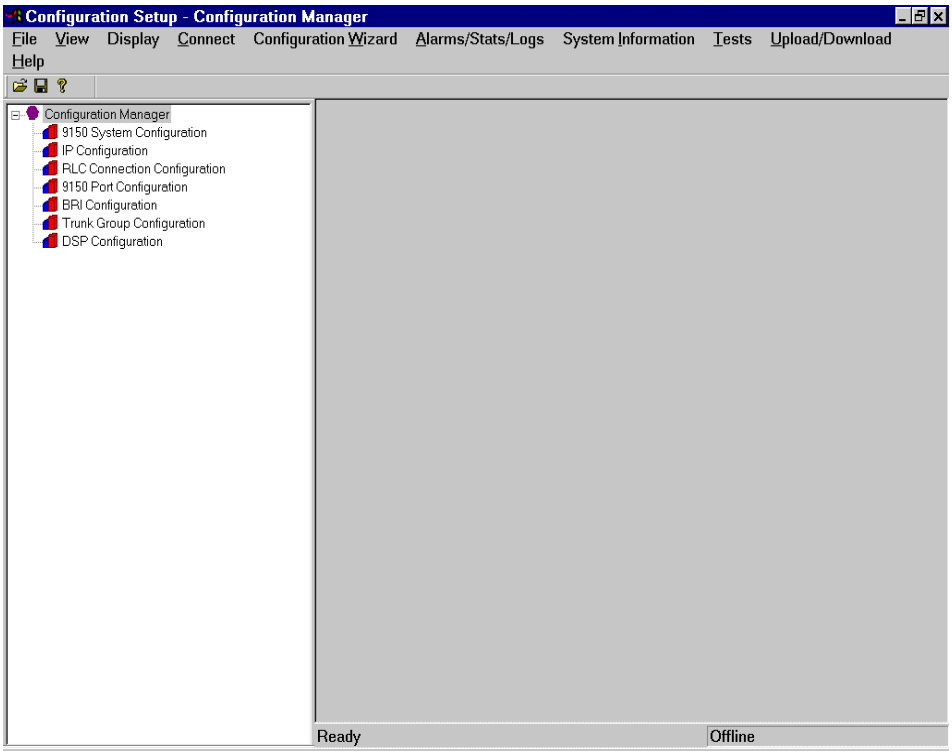
1 Start Configuration Manager as described in “Starting Configuration Manager” on page 164.

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 188.


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.

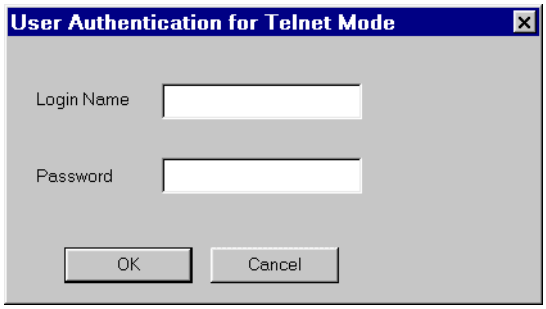
Auto logoff

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.

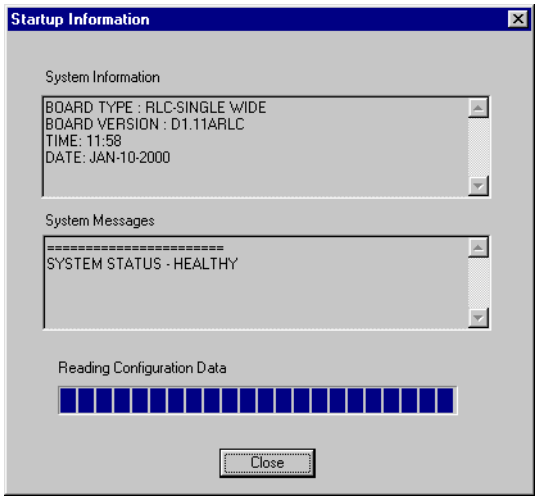
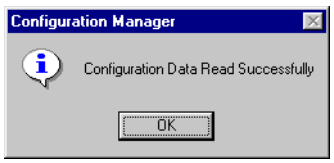
Result: The User Authentication for Telnet Mode dialog box appears.



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.

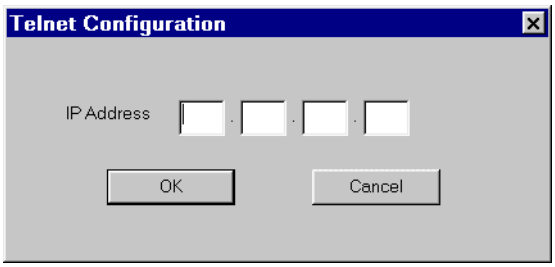
IF the logon attempt	THEN
succeeded	the User Logged In dialog box appears. Click OK. **Result:** The following dialog box appears:  The following messages appear above the progress bar at the bottom of the dialog box: ■ Reading Hardware Information ■ Reading DSP Load Data ■ Reading Configuration Data These messages mean that Configuration Manager is obtaining the unit's configuration information from flash memory. When initialization completes, the following dialog box appears:  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.

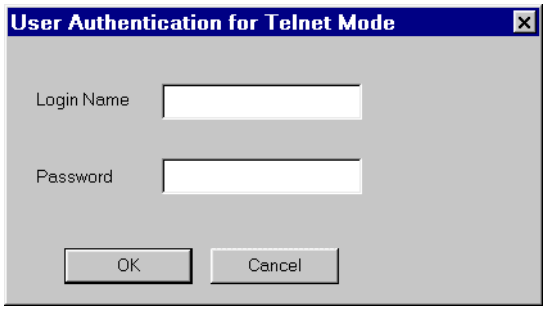
1 From the menu, choose Connect → Login board → Telnet.

Result: The Telnet Configuration dialog box appears.



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

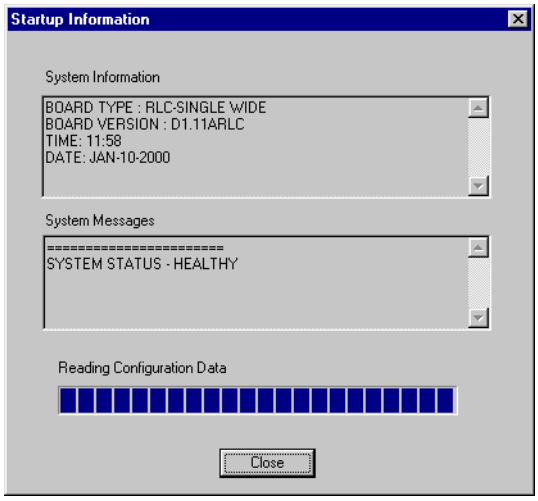
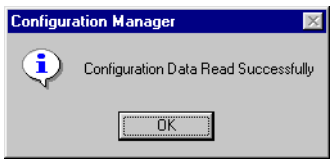
Result: The User Authentication for Telnet Mode dialog box appears.



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.

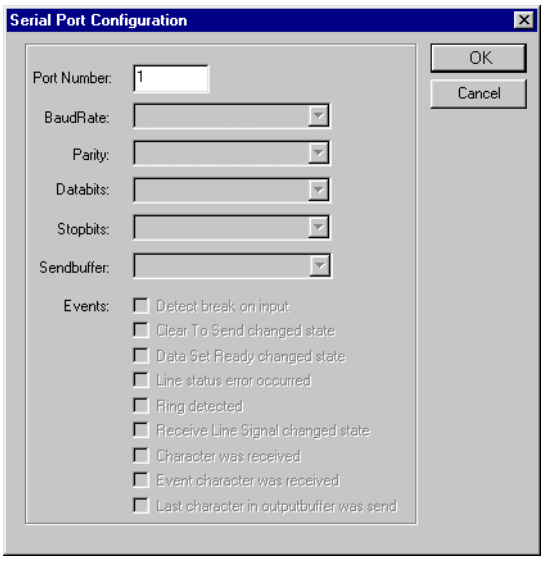
IF the logon attempt	THEN
failed	the following message appears: `10060 TELNET CONNECTION FAILED` Go back to step 1.

IF the logon attempt	THEN
succeeded	the User Logged In dialog box appears. Click OK. **Result:** The following dialog box appears:  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:  Click OK.

To log on to a unit using the serial port

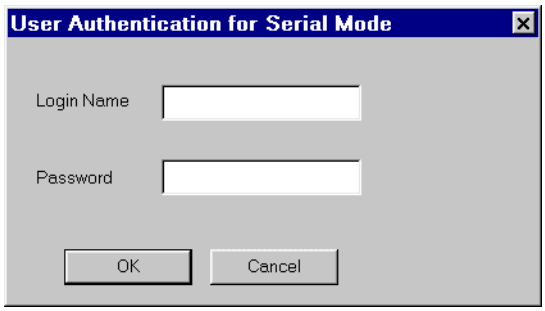
1 From the menu, choose Connect → Login board → Serial.

Result: The Serial Port Configuration dialog box appears.



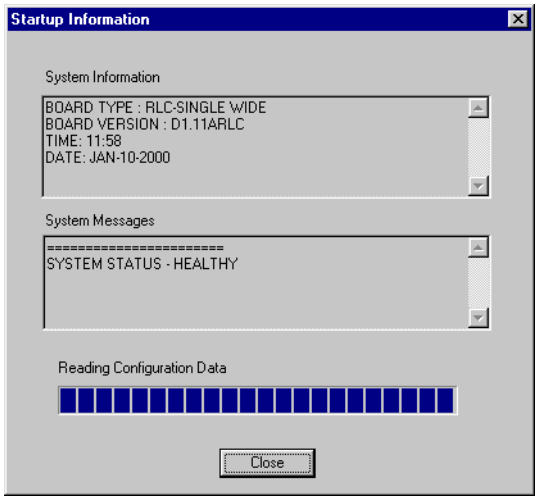
2 Enter the COM port number to which the unit is connected, and then click OK.

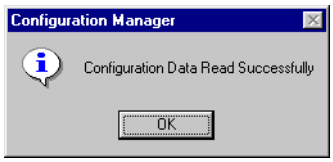
Result: The User Authentication for Serial Mode dialog box appears.



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` Check the serial port connection and ensure it is good. Then, go back to step 1.
succeeded	the User Logged In dialog box appears. Click OK. **Result:** The following dialog box appears:  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:  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

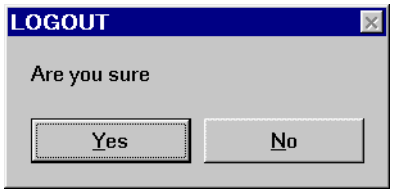
Introduction

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

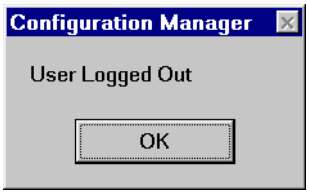
1 From the menu, choose Connect → Logout Board.

Result: The LOGOUT dialog box appears.



2 Click Yes.

Result: The following dialog box appears:



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

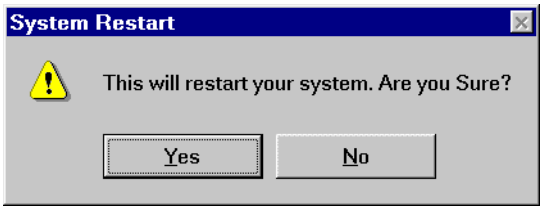
You must perform a system shutdown when

- 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

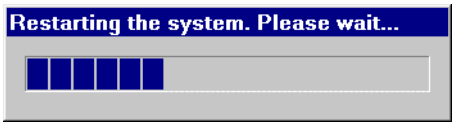
1 From the menu, choose Connect → System Reset → Restart.

Result: The System Restart dialog box appears.



2 Click Yes.

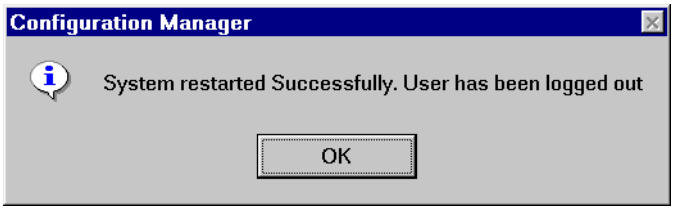
Result: The following status dialog box appears:



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:



3 Click OK.

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

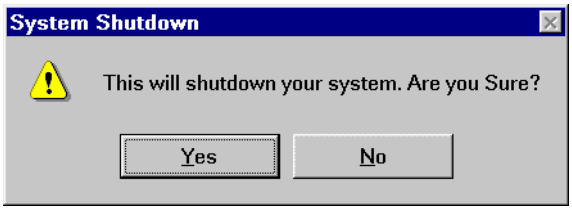
To perform a system shutdown

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.



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 on any property sheet, and then choose Upload/ Download → Save to Flash.
  - Click 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 303.

2 Log off by choosing Connect → Logout Board.

3 From the menu, choose File → Exit.

Result: The Configuration Manager closes.

Chapter 5

Configuring the Remote Office 9150 unit

In this chapter

Overview

Introduction

This chapter describes how to configure the Remote Office 9150 unit so that it can route calls

- over the IP and circuit-switched networks to or from the host PBX
- to or from the local Public Switched Telephone Network (PSTN)

Configuring DSP modules

Each DSP application module that you add to your Remote Office 9150 unit must be configured in Configuration Manager for it to increase your system's call processing capabilities in the ways you intend. This configuration can only take place after the modules have been installed.

IP addresses

To operate as a node on the IP network, the following items must be configured on the Remote Office 9150 unit:

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

These items provide network connectivity between the MIG RLC on the host PBX, the Remote Office 9150 unit in your office, and an administration PC. With this connectivity in place, the following can occur:

- Voice traffic can be routed between the MIG RLC and the Remote Office 9150 unit over the IP network.
- You can use a PC that is located anywhere on the network to connect to and administer the Remote Office 9150 unit (or MIG RLC).

  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.

System settings

The node number and name are settings that uniquely identify each Remote Office 9150 site in the telephone network.

The Remote Office 9150 unit obtains its time and date from the host PBX. If the Remote Office 9150 unit is in a different time zone from the MIG RLC to which it is connected, you can configure the time zone difference.

If your community has implemented an emergency number service (such as 911) to call the police, fire department, or ambulance, and you are using the circuit-switched network to route calls, you can configure the number on the Remote Office 9150 unit. This allows users in your office to dial the emergency number and be connected directly to the local emergency dispatch center without dialing a trunk access code. The call can be made using either the host call appearance or local call appearance keys.

You can enable paging on your Remote Office 9150 unit by doing the following:

- Define a special prefix (SPRE) code for paging.
- Enable the paging feature on each station that needs to use it.

Remote Office 9150 to MIG RLC connection information

Preventing toll fraud

You can implement a security authentication method on both the MIG RLC and the Remote Office 9150 unit to prevent toll fraud.

The security level defines what type of security authentication is used between the Remote Office 9150 unit and the host PBX. The information used to perform security authentication depends on the security level chosen as follows:

- no security
- Caller ID
- security ID

Connection information

Before you can establish a connection to the host PBX site, you must configure the Remote Office 9150 unit to work with the MIG RLC. To accomplish this, specify

- the Remote Office 9150 unit's security ID (if that level of security is used)
- the number used to connect to the host PBX, if you are using the circuit-switched network to route calls
- the trunk used to establish the connection to the host PBX (trunk interface module and B-channel), if you are using the circuit-switched network to route calls

Online/offline mode

The code used to toggle between ISDN BRI online and offline modes is a SPRE code.

When in online mode, calls are directed through the host PBX over either the IP network or circuit-switched network. Long distance charges can apply for calls placed through the PBX over the circuit-switched network.

When in offline mode, calls cannot be made through the host PBX over the IP network or the circuit-switched network. Local calls can still be made through the Public Switched Telephone Network (PSTN) using the ISDN BRI line.

Trunk interface information

A trunk is the straight connection between the PSTN and the Remote Office 9150 unit. Each ISDN BRI line (up to four are supported by the Remote Office 9150 unit) provides two B-channels. In Remote Office 9150 unit context, each B-channel equals one trunk.

Call routing capabilities

You can configure each B-channel on an ISDN BRI line with one of the following call routing capabilities:

- local: The B-channel can route only local calls to and from the local PSTN.
- remote: The B-channel can route calls through the host PBX only.
- local and remote: The B-channel can route calls both to and from the local PSTN and through the host PBX.

Trunk groups

A trunk group consists of one or more B-channels that are grouped logically. You can configure up to eight trunk groups. For example, you could configure

- each B-channel as a different group
- two or more B-channels as a group

Trunk access codes

Trunk access codes are numbers that are used by the Remote Office 9150 unit to determine which trunk group to use when routing the call. You must define a trunk access code for each trunk group.

For example, you can assign trunk access codes #61 and #62, as shown below:

Group 1	Group 2
Trunk 1	Trunk 3
Trunk 2	Trunk 4
Trunk access code: #61	Trunk access code: #62

If a user dials trunk access code #61, the call is routed (or processed) using trunks 1 or 2. If trunks 1 or 2 are both busy, the user's call is blocked (the user receives a fast busy signal).

Permanent versus demand B-channel connection

You can specify whether the trunk connection will be a permanent or demand connection.

A permanent connection means that the ISDN BRI B-channel connection remains open all the time, and should only be used if a flat rate is being charged for ISDN service. A demand connection means that the connection is opened only when you need it.

Stations

To route calls between the host PBX and persons working at the Remote Office 9150 site, you must configure each station at the site on the Remote Office 9150 unit. Each station is associated with a port on the MIG RLC, and can be configured with different capabilities.

If resources on the MIG RLC on the host PBX allow, you can configure up to 32 telephone stations plus one analog device (such as an analog telephone or fax machine). This configuration assumes that none of the stations are equipped with Analog Telephone Adapters (ATAs) or Meridian Communication Adapters (MCAs).

If the ATAs or MCAs will be used to transmit data, the maximum number of ATAs or MCAs that can be supported depends on the type of MIG RLC to which the Remote Office 9150 unit is connected.

MIG RLC type	Maximum number of ATAs or MCAs
single-slot MIG RLC (supporting 16 users)	4
2-slot MIG RLC (supporting 32 users)	7 **Notes:** ■ You can have eight MCAs or ATAs installed if an analog telephone or fax machine is *not* installed. ■ The total number of digital telephones and ATAs cannot exceed 32.

Calling capabilities

You can define each station as a telephone that can process

- local calls only

  Stations defined as *local* can make and receive calls through the local PSTN only and can call other stations at the Remote Office 9150 site. Calls through the host PBX are not allowed.

- remote calls only

  Stations defined as *remote* can make and receive calls through the host PBX only. Calls through the local PSTN are not allowed.

- local and remote calls

  Stations defined as *local and remote* can make and receive calls through both the host PBX and the local PSTN, and can make station-to-station calls at the Remote Office 9150 site.

Call routing

Outgoing calls are routed according to the call appearance key used to initiate the call. Calls initiated on the key defined as the primary or host call appearance key are routed through the host PBX. Calls initiated on the key defined as the local call appearance key are routed through the local PSTN if a trunk access code was dialed before the telephone number.

The Remote Office 9150 unit distinguishes an incoming call by its calling line identification (CLID), and rings it as follows:

- on the host call appearance key if the call was routed through the host PBX
- on the local call appearance key if the call was routed through the local PSTN

Stations and port type

Stations at your site might be configured as one of the following port types on the MIG RLC:

- dedicated port: Each station has sole use of the MIG RLC port to which it is assigned.
- shared (multi-user) port: Up to eight persons can share the same MIG RLC port.

  However, only one person can use the MIG RLC port at any given time. This port type is especially useful for employees who are working in mutually exclusive shifts. All stations that use this type of port respond to the same DN and have identical phoneset configurations.

- dynamic port: This is similar to a multi-user port except that the persons who share ports in a dynamic pool are assigned to the next available port in the pool.

  There is no correlation between the station and the port on the MIG RLC. This feature is especially useful in free-seated ACD environments where agents log on to the host PBX using their agent IDs.

These port types are defined on the MIG RLC. The port type is selected when assigning a station to the MIG RLC port. Your telecom network manager or administrator can tell you which port types apply to your office.

Section A: System settings

In this section

Overview

Introduction

This section describes the settings that apply to the system rather than to the Remote Office 9150 trunks or stations.

System identification information

The unit ID and node name are settings that uniquely identify the MIG RLC and all units that are 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 to 255, which limits the size of your network.

Time and date

The Remote Office 9150 unit obtains its time and date from the host PBX. If the Remote Office 9150 unit is in a different time zone from the MIG RLC to which it is connected, you can configure the time zone difference.

Emergency number

If your community has implemented an emergency number service (such as 911) to call the police, fire department, or ambulance, you can configure that number on the Remote Office 9150 unit. This allows users in your office to dial the emergency number and be connected directly to the local emergency dispatch center through the circuit-switched network. The call is automatically routed through the local Public Switched Telephone Network (PSTN) without having to dial a local trunk access code.

When you configure the local emergency service number on the Remote Office 9150 unit, you also prevent the call from being automatically routed through the host PBX (which could be in a different city from the Remote Office 9150 unit). An emergency call that is routed through the host PBX can result in emergency support being dispatched to the wrong location, which could result in death.

ATTENTION

If you are using only the IP network to route calls, you should make emergency service calls on a telephone that is directly connected to a PSTN line. If you make an emergency service call from a station that is connected to the Remote Office 9150 unit, the call is routed through the host PBX.

Local switchover

You can enable local switchover to automatically route through the Remote Office 9150 unit, the voice path for local station-to-station calls that are made on the host call appearance key.

The signaling data is routed through the host PBX. However, the voice path is routed through the Remote Office 9150 unit to

- prevent tromboning between the MIG RLC and the Remote Office 9150 unit
- save connection bandwidth

Defining SPRE codes

You can define the following SPRE codes for your Remote Office 9150 unit:

- Online and Offline

  The online and offline SPRE codes are used to toggle all stations in your office between online and offline modes.

  Note: When the Remote Office 9150 unit is in offline mode, you cannot make calls through the host PBX over the IP or circuit-switched network.

  - To go online, dial the Online SPRE code on any station. When in online mode, calls are directed through the host PBX. Any long distance charges associated with calls placed through the PBX are charged to your organization.

- To go offline, dial the Offline SPRE code on any station. When in offline mode, only calls that are directed through the Public Switched Telephone Network (PSTN) are allowed.

Note: See also “Going online and offline” on page 289.

- Paging

  A page is a broadcast announcement from one station to all other stations at the Remote Office 9150 unit site. You can enable paging on your Remote Office 9150 unit by doing the following:

  - Define a SPRE code for paging.
  - Enable the paging feature on each station that needs to use it.

  To send a page to the speaker of all stations at your site, dial the paging SPRE code on any paging-enabled station.

- Local Calling

  If an analog or ATA-equipped station is defined with local and remote calling capability, and it goes off-hook to make an outgoing call, then the outgoing call is automatically a host-controlled call. The station user can switch the call to local-controlled mode by dialing the Local Calling SPRE code before the telephone number.

- Registration and Deregistration

  A station user uses the registration SPRE code to register with a multi-user or dynamic port.

  The deregistration SPRE code disengages the user from the port so that another user can use it. The user is put into *not logged in* mode.

Note: All SPRE codes are automatically defined in Configuration Manager with a pound prefix (# in North America) so that there are no conflicts with host PBX dialing plans. SPRE codes must be between 1 and three digits in length in addition to the pound sign.

For a list of the default SPRE codes, refer to the “Remote Office 9150 Configuration Information—Dialing Plans” form on page 436.

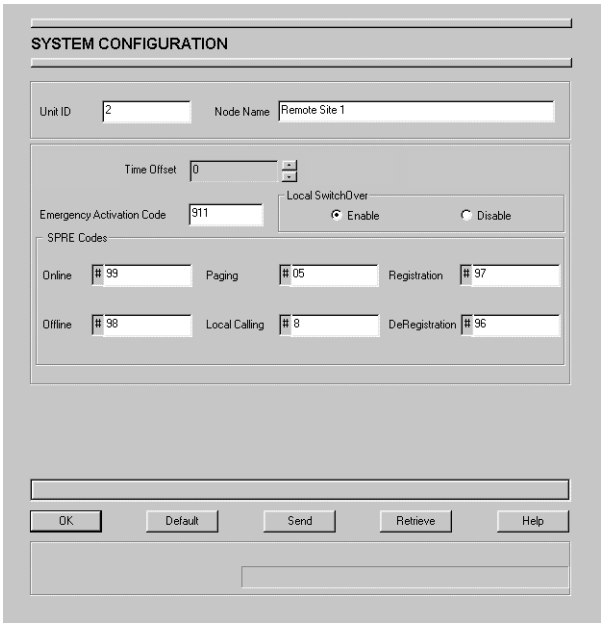
Configuring the system settings

Introduction

This section describes the settings that apply to the system rather than to the MIG RLC port or Remote Office 9150 trunks or stations.

Getting there 9150 → Configuration Manager → 9150 System Configuration

System Configuration sheet



To configure the Remote Office 9150 system settings

1 Complete the fields as described in “9150 System Configuration field descriptions” on page 217.

2 Click OK to save the information in the temporary work file.

3 To update the Remote Office 9150 unit with the new information, click Send.

IF you are	THEN
logged on to the Remote Office 9150 unit	the changes are written into the Remote Office 9150 unit’s buffer. To save the changes in flash memory, choose Upload/Download → Save to Flash.
not logged on to the Remote Office 9150 unit	the following dialog box appears:  Do one of the following: ■ Log on to the Remote Office 9150 unit, and then click Send again. ■ Save the changes to a file on your administration PC.

9150 System Configuration field descriptions

Field	Description
Unit ID	Assign a number between 1 and 255 to the Remote Office 9150 unit that you are configuring. 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
Node Name	Enter your site name. The node name uniquely identifies this Remote Office 9150 site in the telephone network.
Time Offset	Click the up or down arrows to define the time zone difference from the host PBX. **Note:** The time can be changed in 15-minute intervals only.
Emergency Activation Code	If you are using the circuit-switched network to route calls, then enter the number your community dials to reach an emergency service. If you are using only the IP network to route calls, leave this field blank.

Field	Description
Local SwitchOver	Select Enable to automatically route through the Remote Office 9150 unit, the voice path for local station-to-station calls that are made on the host call appearance key. The signaling data is routed through the host PBX. However, the voice path is routed through the Remote Office 9150 unit to ■ prevent tromboning between the MIG RLC and Remote Office 9150 unit ■ save connection bandwidth Select Disable to route the voice path through the PBX.
SPRE Codes: Online	Enter the SPRE code that is used to put your site into online mode, or accept the default. The default is #99. **Note:** The SPRE code is automatically prefixed with the pound sign (# in North America). This means users must dial # before the SPRE code when going into online mode. Maximum length: 3 digits in addition to the pound sign
SPRE Codes: Paging	Enter the SPRE code that is used to announce pages to other stations in your office, or accept the default code. The default is #05. **Note:** The SPRE code is automatically prefixed with a pound sign (#). This means users must dial # before the SPRE code when initiating a page. Maximum length: 3 digits in addition to the pound sign

Field	Description
SPRE Codes: Registration	Enter the SPRE code that is used to register a user with a multi-user or dynamic port, or accept the default code. The default is #97. **Note:** The SPRE code is automatically prefixed with a pound sign (#). This means users must dial # before the SPRE code when registering for a port. Maximum length: 3 digits in addition to the pound sign
SPRE Codes: Offline	Enter the SPRE code that is used to put your site into offline mode, or accept the default code. The default is #98. **Note:** The SPRE code is automatically prefixed with the pound sign (# in North America). This means users must dial # before the SPRE code when going into offline mode. Maximum length: 3 digits in addition to the pound sign
SPRE Codes: Local Calling	Enter the SPRE code that allows analog or ATA-equipped station users to change the outgoing call mode to local-controlled mode. The default is #8. **Note:** The SPRE code is automatically prefixed with a pound sign (#). This means users must dial # before the SPRE code when initiating a local call on an analog or ATA-equipped station. Maximum length: 3 digits in addition to the pound sign
SPRE Codes: DeRegistration	Enter the SPRE code that is used to disengage the user from a multi-user or dynamic port, or accept the default code. The default is #96. **Note:** The SPRE code is automatically prefixed with a pound sign (#). This means users must dial # before the SPRE code when disengaging from a port. Maximum length: 3 digits in addition to the pound sign

Section B: IP addresses

In this section

About IP addresses

Introduction

To operate as a node on the IP network, the following items must be configured on the Remote Office 9150 unit:

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

These items provide network connectivity between the MIG RLC on the host PBX, the Remote Office 9150 unit in your office, and an administration PC. With this connectivity in place, the following can occur:

- Voice traffic can be routed between the MIG RLC and the Remote Office 9150 unit over the IP network.
- You can use a PC that is located anywhere on the network to connect to the Remote Office 9150 unit (or MIG RLC).

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

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 dotted decimal notation (for example, 123.45.67.89).

The IP address assigned to the Remote Office 9150 unit must be unique, and 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.

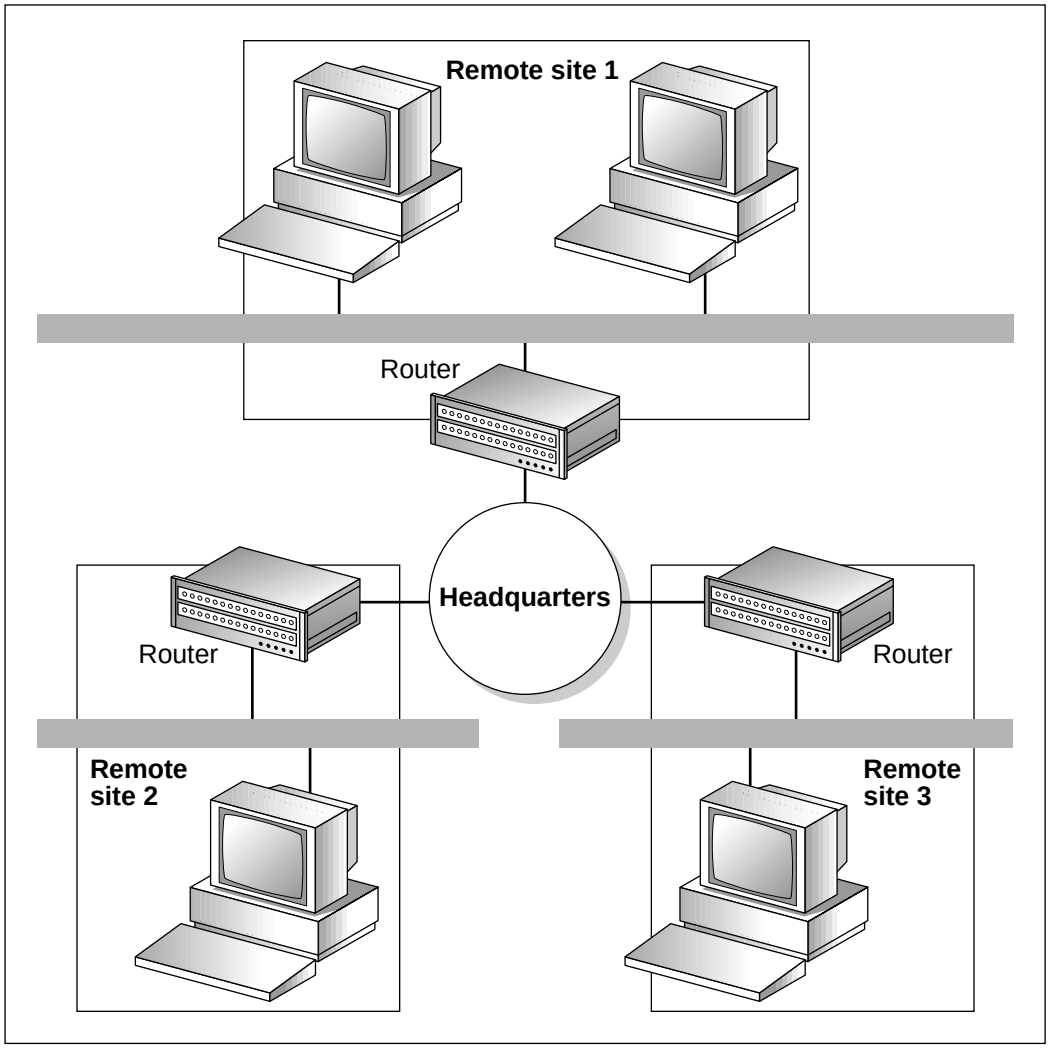
What is a subnet mask?

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 Remote Office 9150 unit, what portion of the IP address represents the network (and subnetwork), and what portion represents the host.

Example of subnet use

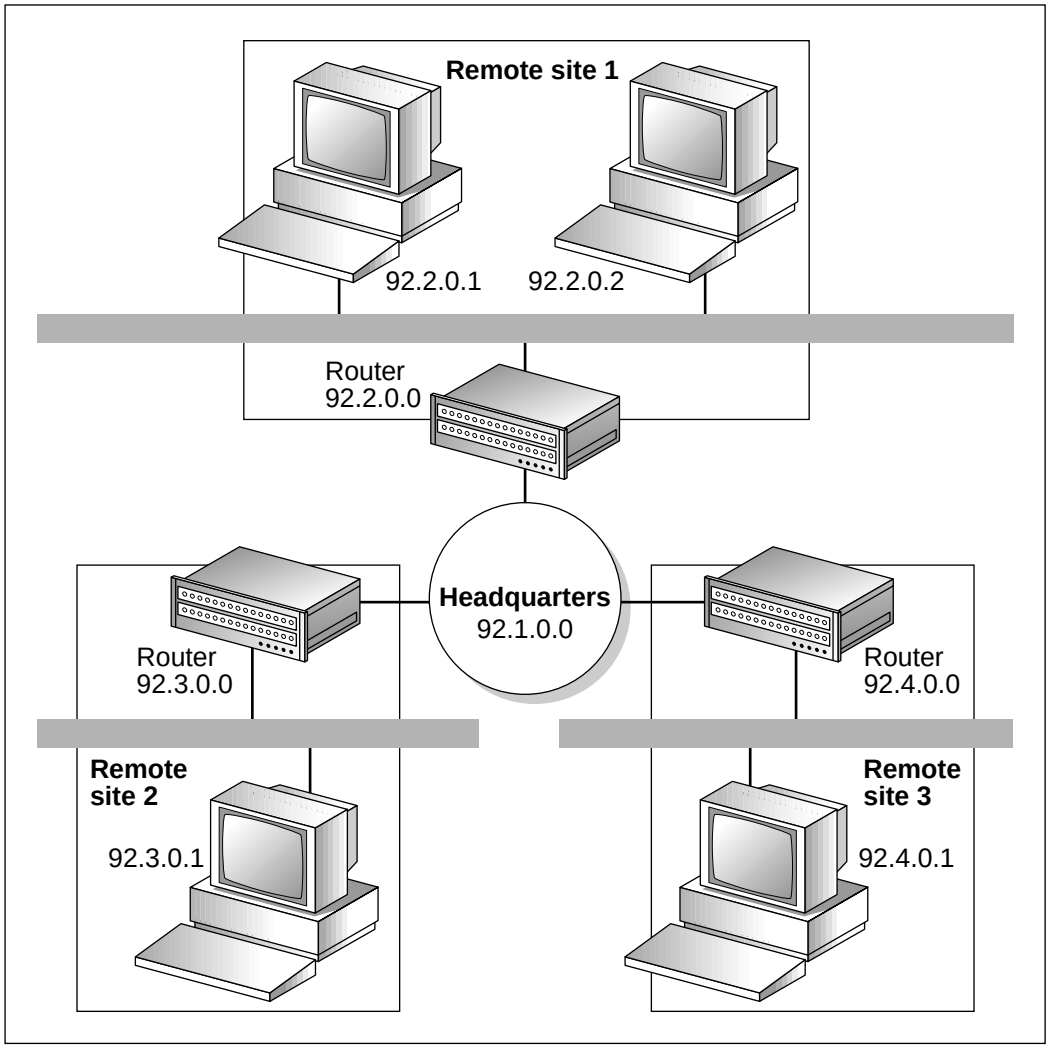
The following illustration shows a typical setup for an organization with headquarters and branch offices.

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 is very expensive. It is possible to use a different network for each office, but this is also expensive.



G101483

Subnets offer a solution to this problem. In the illustration on the next page, 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. When it is configured on the Remote Office 9150 unit, this tells the Remote Office 9150 unit that the first 16 bits of the IP address represent the network and subnetwork.

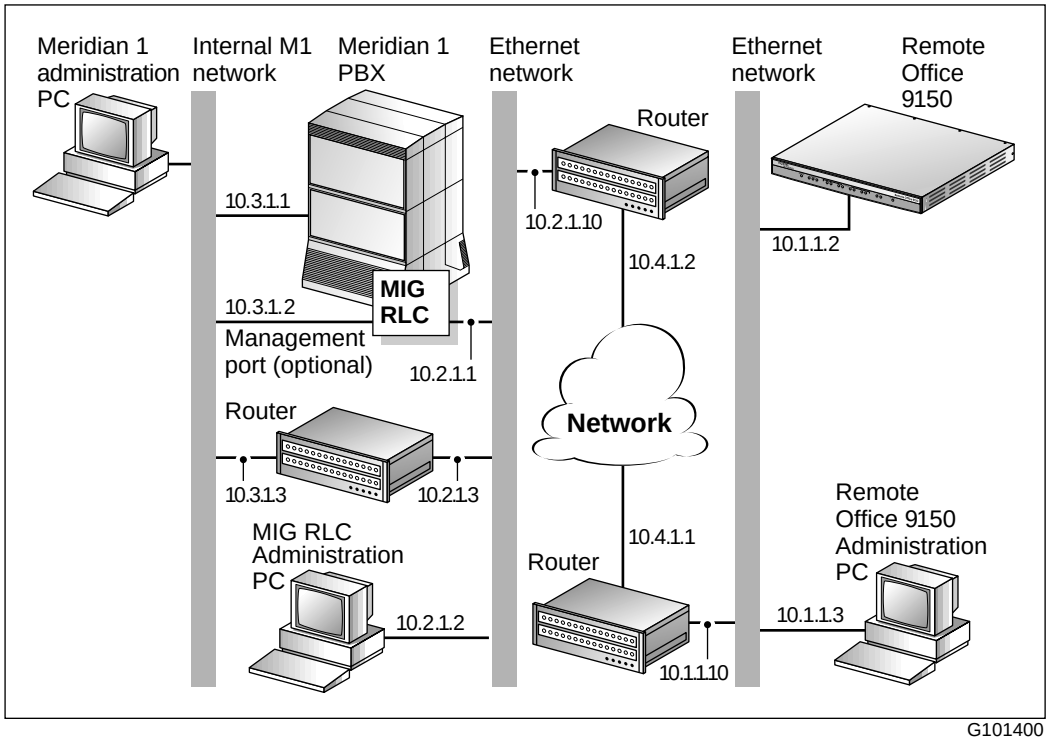
Default gateway

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

In a Remote Office 9150 context, the gateway is the device on the network that directs traffic to and from the Remote Office 9150 unit.

Remote Office 9150 unit position in your IP network

As discussed earlier in this guide, the Remote Office 9150 unit is connected to a hub on your IP network. The following diagram provides an example of what the network looks like.



Configuring the Remote Office 9150 unit's IP interface

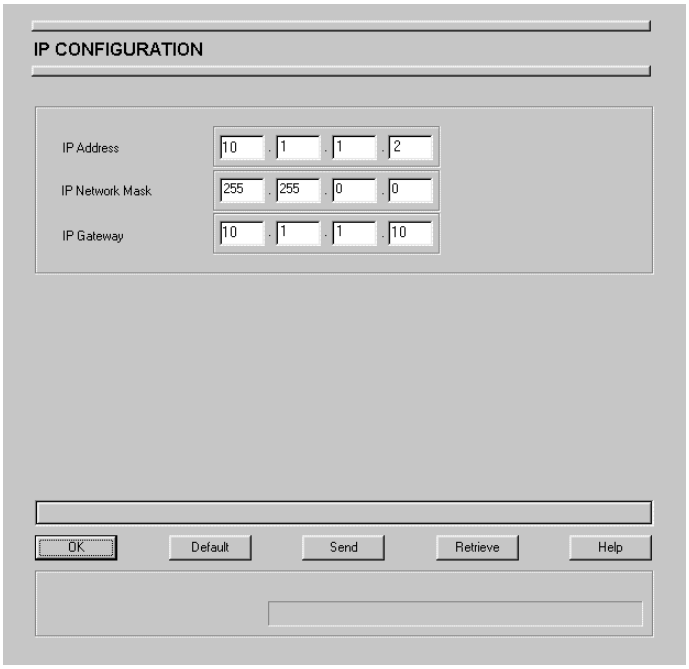
Introduction

This section explains how to enter the IP address, subnet mask, and default gateway for the Remote Office 9150 unit.

For a description of each of these items, see "About IP addresses" on page 222.

Getting there 9150 → Configuration Manager → IP Configuration

IP Configuration sheet



To enter the IP addresses

1 Enter the IP address assigned to the Remote Office 9150 unit into the IP Address boxes.

2 Enter the subnet mask into the IP Network Mask boxes.

3 Enter the IP address of the network gateway into the IP Gateway boxes.

4 Click OK to save the information in the temporary work file.

5 To update the Remote Office 9150 unit with the new information, click Send.

IF you are	THEN
logged on to the Remote Office 9150 unit	the changes are written into the Remote Office 9150 unit's buffer. To save the changes in flash memory, choose Upload/Download → Save to Flash.
not logged on to the Remote Office 9150 unit	the following dialog box appears:  Do one of the following: ■ Log on to the Remote Office 9150 unit, and then click Send again. ■ Save the changes to a file on your administration PC.

6 Restart the Remote Office 9150 unit.

Note: For instructions on how to restart the Remote Office 9150 unit, see "Performing a system restart or shutdown" on page 198.

Section C: RLC connection information

In this section

Overview

Introduction

This section shows you how to configure your Remote Office 9150 unit to connect with the MIG RLC on the host PBX.

RLC connection information

Before you can establish a connection to the host PBX, you must configure the Remote Office 9150 unit to work with the MIG RLC. To accomplish this, you must specify

- the PSTN number used to connect to the host PBX, if you are using the circuit-switched network to route calls
- the IP address of the MIG RLC, if you are using the IP network to route calls
- whether you want to enable Block Incoming Local Call on Primary B Channel

Security level

You can implement a security authentication method on both the MIG RLC and the Remote Office 9150 unit to prevent toll fraud.

The security level defines what type of security authentication is used between the Remote Office 9150 unit and the host PBX. The information used to perform security authentication depends on the security level chosen as follows:

- no security
- calling line identification

  Note: On the Remote Office 9150 unit, this is referred to as *Caller ID*.
- security identifier

  Note: On the Remote Office 9150 unit, this is referred to as *Provision ID*.

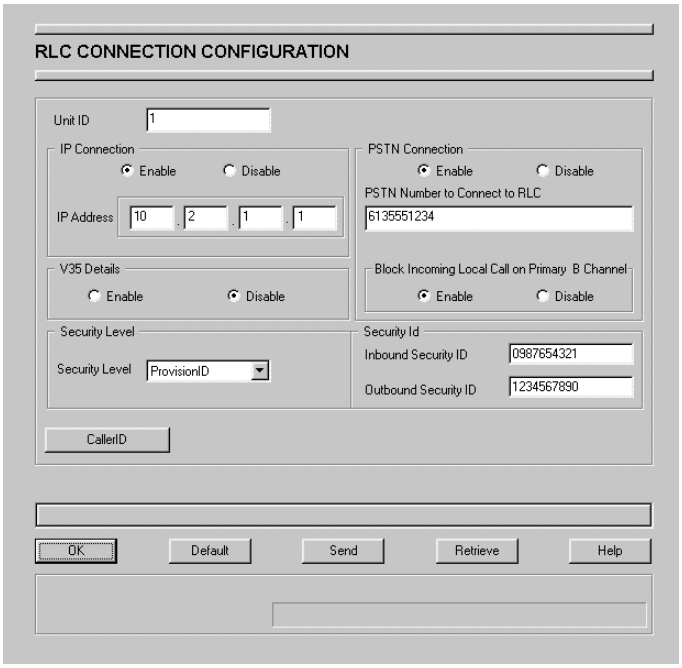
Configuring the RLC connection information

Introduction

This section describes how to configure information needed by the Remote Office 9150 unit to establish connections with the MIG RLC on the host PBX.

Getting there 9150 → Configuration Manager → RLC Connection Configuration

RLC Connection Configuration sheet



To configure the RLC connection information

1 Complete the fields as described in “RLC Connection Configuration field descriptions” on page 233.

2 Click OK to save the information in the temporary work file.

3 To update the Remote Office 9150 unit with the new information, click Send.

IF you are	THEN
logged on to the Remote Office 9150 unit	the changes are written into the Remote Office 9150 unit’s buffer. To save the changes in flash memory, choose Upload/Download → Save to Flash.
not logged on to the Remote Office 9150 unit	the following dialog box appears:  Do one of the following: ■ Log on to the Remote Office 9150 unit, and then click Send again. ■ Save the changes to a file on your administration PC.

RLC Connection Configuration field descriptions

Field	Description
Unit ID	Enter the number (between 1 and 255) assigned to the MIG RLC to which this Remote Office 9150 unit is connected. The MIG RLC's unit ID must be different from ■ this Remote Office 9150 unit's ID ■ the IDs of other units that are also connected to the MIG RLC **Note:** This Unit ID must be entered on the Remote Connection Configuration property sheet on the MIG RLC to create the communication path between this Remote Office 9150 unit and the MIG RLC.
IP Connection	Select Enable if you want to route calls over your IP network. Select Disable if you do not want to route calls over your IP network.
PSTN Connection	Select Enable if you want to route calls over the circuit-switched network. Select Disable if you do not want to route calls over the circuit-switched network.
IP Address	Enter the MIG RLC's IP address. The Remote Office 9150 unit will use this IP address to connect to the MIG RLC over the IP network.

Field	Description
PSTN Number to Connect to RLC	If you enabled the PSTN connection, enter the telephone number used to connect to the MIG RLC. The telephone number can contain the following digits and characters: 0 through 9, #, *, comma (,), period (.), and dash (-). ■ Caller ID separator: “.” (period) ■ Caller ID separator and 1/2-second delay: “,” (comma) ■ null separator: “-” (dash) **Note:** If the Caller ID security level is selected, the telephone number configured here is compared with the telephone number configured on the MIG RLC for your site. If the two numbers do not match, the call is dropped.
V35 Details	V.35 is for future use. It is not supported in this release.
Block Incoming Local Call on Primary B Channel	Select Enable if incoming local calls *should not* be received on the first B-channel. Select Disable if the first B-channel *should* receive incoming local calls.

Configuring the security level

Introduction

It is recommended that you implement a security authentication method on both the MIG RLC and the Remote Office 9150 unit to prevent toll fraud.

The security level defines what type of security authentication is used between the Remote Office 9150 unit and the host PBX. The information used to perform security authentication depends on the security level chosen.

No security

When no security is being used, the MIG RLC and Remote Office 9150 unit do not perform a security check. All connection attempts to the host PBX and Remote Office 9150 unit are allowed.

Caller ID

When you select Caller ID, you can define the valid Caller IDs that the Remote Office 9150 unit can receive. If the Caller ID on the incoming call matches what is configured on the Remote Office 9150 unit, the connection is established. If it does not match, the call is dropped.

Note: Caller ID cannot be performed over the IP network. Caller ID authentication can be used only on the circuit-switched network.

Security identifier

You can use security identifier authentication over the IP or circuit-switched network. If you select this security level, security identifiers must be configured on both the Remote Office 9150 unit and the MIG RLC port to which the unit is assigned. When a connection to or from the host PBX is attempted, the security identifiers are compared. If they match, the connection is established. If they do not match, the call is dropped.

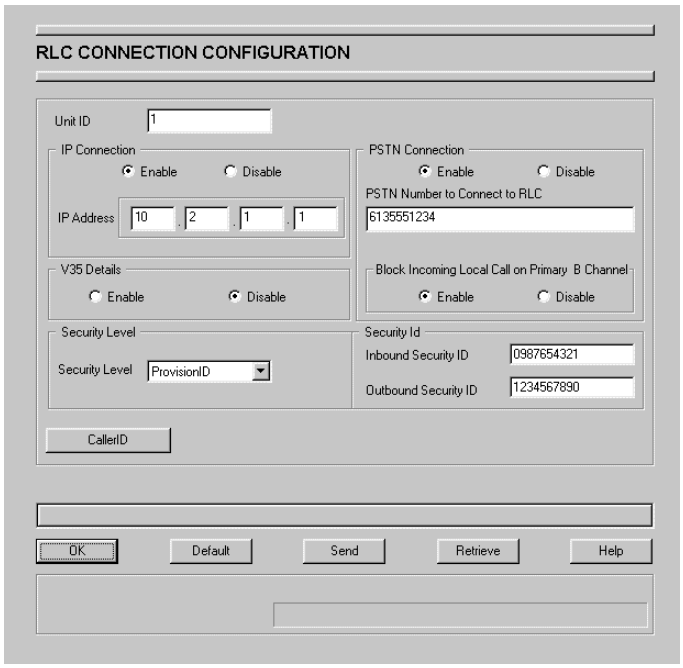
You must configure two security identifiers on the Remote Office 9150 unit:

- inbound security identifier: This is the MIG RLC's security identifier. It is presented on incoming calls.
- outbound security identifier: This is the Remote Office 9150 unit's security identifier. It is presented to the MIG RLC on outgoing calls.

You must configure the same security identifiers in reverse on the MIG RLC port to which this Remote Office 9150 unit is assigned.

Getting there 9150 → Configuration Manager → RLC Connection Configuration

RLC Connection Configuration sheet

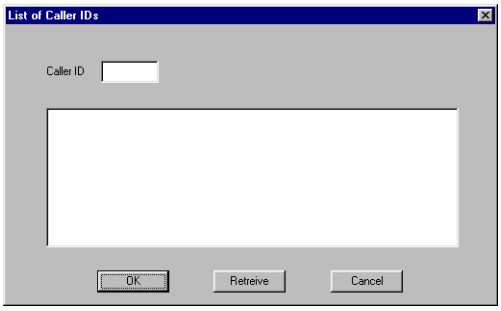


To configure the security level

1 Select one of the following security level settings from the Security Level list box:

- No Security
- Caller ID
- Provision ID

2 If you selected Caller ID or Provision ID security levels, do one of the following:

IF you selected	THEN
Caller ID	click CallerID. **Result:** The List of Caller IDs dialog box appears.  In the Caller ID box, enter the telephone number from which the Remote Office 9150 unit can accept calls. Ensure that the telephone number you enter matches the Caller ID actually presented by the MIG RLC. Click OK, and then click Add from the pop-up menu that appears. **Result:** The telephone number appears in the blank box.

IF you selected	THEN
Provision ID	the Security ID fields are enabled. Do the following: ■ Enter the MIG RLC's security identifier (up to 10 digits in length) in the Inbound Security ID field. ■ Enter the Remote Office 9150 unit's security identifier (up to 10 digits in length) in the Outbound Security ID field.

3 Click OK to save the information in the temporary work file.

4 To update the Remote Office 9150 unit with the new information, click Send.

IF you are	THEN
logged on to the Remote Office 9150 unit	the changes are written into the Remote Office 9150 unit's buffer. To save the changes in flash memory, choose Upload/Download → Save to Flash.
not logged on to the Remote Office 9150 unit	the following dialog box appears:  Do one of the following: ■ Log on to the Remote Office 9150 unit, and then click Send again. ■ Save the changes to a file on your administration PC.

Section D: Trunk interface information

In this section

About trunks and trunk groups

Introduction

This section shows you how to configure your trunks to connect with the MIG RLC at the host site, or to make calls through the local PSTN.

Trunks

A trunk is the straight connection between the PSTN and the Remote Office 9150 unit. Each ISDN BRI line (up to four are supported by the Remote Office 9150 unit) provides two B-channels. In Remote Office 9150 unit context, each B-channel equals one trunk.

Each B-channel is defined as follows:

- as a local trunk, remote trunk, or both
- as a permanent or demand connection

Local trunk

The trunk is used to make local calls over the PSTN.

Remote trunk

A remote trunk is used to establish a connection to the MIG RLC from the Remote Office 9150 unit.

Local and remote trunk

A B-channel that is defined as both local and remote can be used to make calls through both the local PSTN, as well as through the MIG RLC on the host PBX.

Permanent versus demand connection

You can also specify whether the trunk connection will be a permanent or demand connection.

A permanent connection means that the ISDN BRI B-channel connection remains open all the time, and should only be used if a flat rate is being charged for ISDN service. A demand connection means that the connection is opened only when you need it.

Trunk groups

A trunk group consists of one or more B-channels that are logically grouped. You can configure up to eight trunk groups. For example, you can configure

- each B-channel as a different trunk group
- two or more B-channels as a trunk group

A B-channel can be a member of more than one trunk group.

Trunk access codes

Trunk access codes are numbers that are used by the Remote Office 9150 unit to determine which trunk group to use when routing the call. You must define a trunk access code for each trunk group.

For example, you can assign trunk access codes #61 and #62, as shown below:

Group 1	Group 2
Trunk 1	Trunk 3
Trunk 2	Trunk 4
Trunk access code: #61	Trunk access code: #62

If a user dials trunk access code #61, the call is routed (or processed) using trunks 1 or 2. If trunks 1 and 2 are both busy, the user's call is blocked (the user receives a fast busy signal).

Note: All trunk access codes are automatically defined in Configuration Manager with a pound prefix (# in North America) so that there are no conflicts with host PBX dialing plans. Trunk access codes must be between one and three digits in length in addition to the pound sign.

For a list of the default trunk access codes, refer to the "Remote Office 9150 Configuration Information—Dialing Plans on page 436.

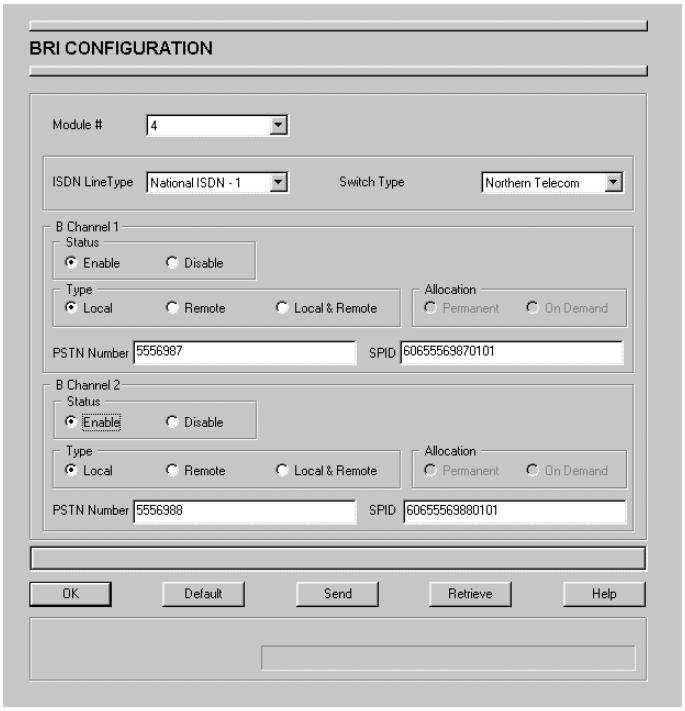
Configuring BRI trunks

Introduction

This topic shows you how to configure the BRI trunks. See “About trunks and trunk groups” on page 240 for a detailed explanation of BRI configuration settings.

Getting there 9150 → Configuration Manager → BRI Configuration

BRI Configuration sheet



To enter the BRI settings

1 Complete the fields as described in “BRI Configuration field descriptions” on page 244.

2 Click OK to save the information in the temporary work file.

3 To update the Remote Office 9150 unit with the new information, click Send.

IF you are	THEN
logged on to the Remote Office 9150 unit	the changes are written into the Remote Office 9150 unit’s buffer. To save the changes in flash memory, choose Upload/Download → Save to Flash.
not logged on to the Remote Office 9150 unit	the following dialog box appears:  Do one of the following: ■ Log on to the Remote Office 9150 unit, and then click Send again. ■ Save the changes to a file on your administration PC.

BRI Configuration field descriptions

Field	Description
Module #	Select the number identifying the trunk interface module that you are configuring. **Note:** The number you select must match the module position where the module has been installed. Valid options: 4 through 7
ISDN Line Type	Select the ISDN variant used in your country. Get this information from your ISDN service provider.
Switch Type	Select the type of switch used by your ISDN service provider for this trunk. Get this information from your ISDN service provider.
Status (B channel 1 and B channel 2)	Select Enable to activate the ISDN BRI channel. Select Disable to deactivate it.
Type (B channel 1 and B channel 2)	Select the type of connection—local, remote, or local and remote. ■ Local: This trunk is used for local PSTN calls only. ■ Remote: This trunk creates a circuit-switched connection path to the host PBX. ■ Local & Remote: This trunk can route local PSTN calls and host PBX calls. **Note:** If you select Local or Local & Remote, then the Allocation field is enabled.
Allocation (B channel 1 and B channel 2)	Select Permanent if you want the connection to remain open all the time. Select On Demand to activate the connection only when needed.

Field	Description
PSTN Number (B channel 1 and B channel 2)	Enter the full telephone number provided to you by your ISDN service provider for this B-channel. Include access codes, dialing prefix, and area code if necessary. When entering the area code, always enter it directly before the main telephone number. Do not use a hyphen (-) as a separator because hyphens are reserved for subaddressing.
SPID (B channel 1 and B channel 2)	Enter the Service Profile Identifier (SPID) provided to you by your ISDN service provider for this B-channel.

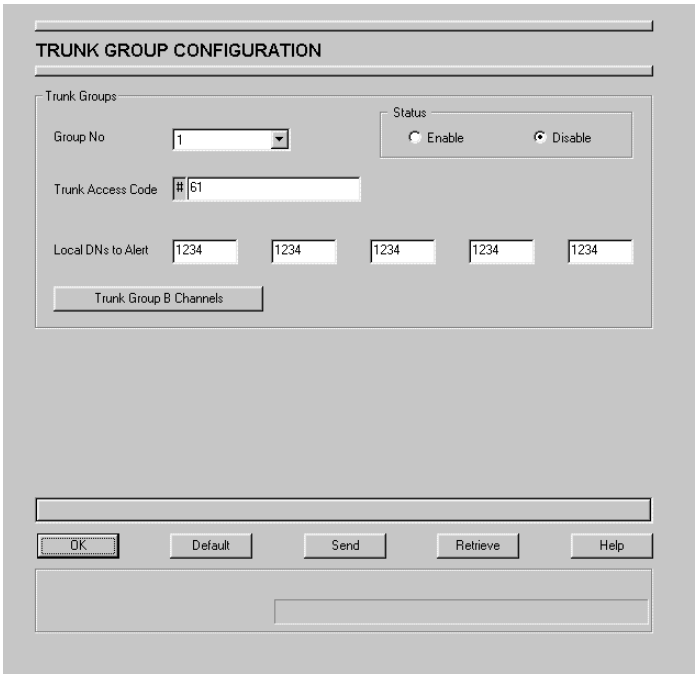
Configuring trunk groups

Introduction

This section shows you how to enable and create trunk groups for use with the Remote Office 9150 unit. For more information, see “Trunk groups” and “Trunk access codes” on page 241.

Getting there 9150 → Configuration Manager → Trunk Group Configuration

Trunk Group Configuration sheet



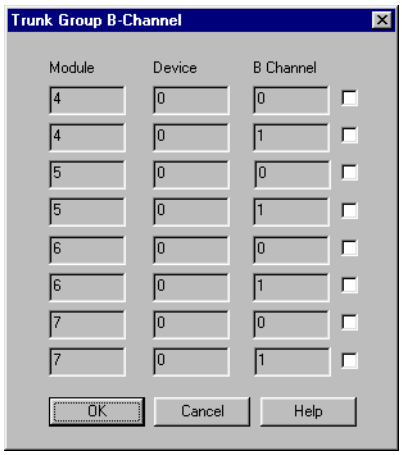
To configure trunk groups

1. Complete the fields as described in “Trunk Group Configuration field descriptions” below.
2. Click OK to save the information in the temporary work file.
3. To update the Remote Office 9150 unit with the new information, click Send.

IF you are	THEN
logged on to the Remote Office 9150 unit	the changes are written into the Remote Office 9150 unit’s buffer. To save the changes in flash memory, choose Upload/Download → Save to Flash.
not logged on to the Remote Office 9150 unit	the following dialog box appears:  Do one of the following: ■ Log on to the Remote Office 9150 unit, and then click Send again. ■ Save the changes to a file on your administration PC.

Trunk Group Configuration field descriptions

Field	Description
Group No	Select a group number. You can create up to ten groups.
Status	Select Enable to activate the trunk group. Select Disable to deactivate the trunk group.

Field	Description
Trunk Access Code	Enter the trunk access code that you want to assign to the trunk group, or accept the default. **Note:** The trunk access code is automatically prefixed with a pound sign (# in North America). This means users must dial the # before the trunk access code when making an outgoing local call. Maximum length: 1 to 3 digits in addition to the pound sign
Local DNs to Alert	If you want incoming calls to ring on specific telephones only, then enter the DNs of those telephones. If you leave the fields blank, then incoming calls received by this trunk group ring on all telephones.
Trunk Group B Channels	Click Trunk Group B Channels. **Result:** The Trunk Group B-Channel dialog box appears. 

Field	Description
Trunk Group B Channels (continued)	Complete the fields as follows: ■ Module: Displays trunk interface module numbers. ■ Device: Displays the internal device number for each B-channel provided by the module. ■ B Channel: Displays B-channel numbers. ■ Check boxes: Click the check box for each B-channel you want to include in this trunk group. **Note:** A B-channel can be a member of more than one trunk group. Click OK.

Section E: Stations

In this section

Station overview

Introduction

This section explains how to configure the Remote Office 9150 unit so that it can

- route calls between the stations at your site and the host PBX

  Each station is associated with a port on the MIG RLC, and can be configured with different capabilities.
- make calls through the local PSTN or to other stations at the Remote Office 9150 site

If resources on the MIG RLC on the host PBX allow, you can configure up to 32 telephone stations plus one analog device (such as an analog telephone or fax machine). This configuration assumes that none of the stations are equipped with Analog Telephone Adapters (ATAs) or Meridian Communication Adapters (MCAs).

Call processing capabilities and station settings

Each station can be defined as a telephone that can process

- local calls only
- remote calls only
- local and remote calls

Stations defined with local call capability are further defined with telephone features and local call appearance keys. Stations that are defined with remote call capability do not need to be further configured because they inherit their features and call appearance keys from their associated port configurations on the host PBX.

Local call capability

Stations defined as *local* can make and receive calls through the local PSTN or to other stations at the Remote Office 9150 site. Calls through the host PBX are not allowed.

Local stations are not associated with MIG RLC ports.

Remote call capability

Stations defined as *remote* are associated with MIG RLC ports, and can make and receive calls through the host PBX only. Calls through the local PSTN are not allowed.

Local and remote call capability

Stations defined as *local and remote* are associated with MIG RLC ports, and can

- make and receive calls through both the host PBX and the local PSTN
- make calls to other stations at the Remote Office 9150 site

Outgoing calls are routed according to the call appearance key used to initiate the call.

- Calls initiated on the key defined as the host call appearance key (also referred to as the *primary DN key*) are routed through the host PBX.
- External calls initiated on the key defined as the local call appearance key are routed through the local PSTN.
- Internal calls initiated on the local call appearance key are routed to other stations at the Remote Office 9150 site.

The Remote Office 9150 unit distinguishes an incoming call by its calling line identification, and rings it as follows:

- on the host call appearance key if the call was routed through the host PBX
- on the local call appearance key if the call was routed through the local PSTN or if the call was a station-to-station call

Local station settings

When a station is defined with local capability, you can further configure the station to

- enable or disable certain features (for more details, see “Defining stations” on page 260)
- disable outgoing dialing digit sequences (see “Disabled Outbound Digit Seq.” on page 263)
- identify local call appearance and feature key positions (see “Optional Feature Keys” on page 264)

Remote station settings

When the station is defined with remote capability, you can assign it to a specific port on the MIG RLC (see “Defining stations” on page 260).

Call appearance keys

The host call appearance key is defined for each station on the host PBX. It is not defined for each station on the Remote Office 9150 unit.

The local call appearance keys, on the other hand, must be defined for each station connected to the Remote Office 9150 unit to allow

- users to make outgoing calls using Remote Office 9150 trunks
- users to make station-to-station calls without host PBX control
- incoming calls on Remote Office 9150 trunks to ring specific stations

The local call appearance keys must be left undefined in the host PBX configuration to avoid indicator conflicts between the host PBX and the Remote Office 9150 unit. Only indicators defined as local call appearances are blocked from the host PBX.

When to configure the local call appearance keys

The local call appearance key positions must be defined when a new station is being configured with local capability, or when a request to change feature key positions has been initiated.

Associating trunk groups with local stations

Each trunk group can be defined to ring only specific stations. This feature allows you to route certain types of calls (such as incoming calls on a 1-800 number) to specific stations.

Private lines

A private line is a telephone line that is used by one person only. Calls that are routed to the private line do not ring on any other station in your office. To dedicate a private line to a station, configure a trunk group to ring incoming calls only on that station.

If you are connecting a fax machine to the Remote Office 9150 unit, then configure a private line to the fax. Incoming calls on this line are routed directly to the fax.

For instructions, refer to “Configuring trunk groups” on page 246.

Calling permissions and restrictions

You can consider the ability to make certain types of calls from a station to be a calling permission. Similarly, a certain type of call that is not allowed is a calling restriction.

You can define both permissions and restrictions for each station.

Local and remote calling permissions

When you define a station as a local station, you are granting the station with local calling permission. Calls can be made or received through the local PSTN or to and from other stations. Calls through the host PBX are not allowed.

When you define a station as a remote station, you are granting the station with remote calling permission. Calls can be made or received through the host PBX only. Calls through the local PSTN are not allowed.

Exception: If the emergency service number is configured on the Remote Office 9150 unit and you are using the circuit-switched network to route calls, the dialed emergency service number is routed through the local PSTN to the emergency service. This ensures that the emergency service receives the correct calling location information.

When you define a station as a local and remote station, you are granting the station with the ability to make or receive calls through both the local PSTN and the host PBX. Station-to-station calls are also allowed.

Call restriction

You can prevent certain types of calls from being made at a station by disabling the digits that normally allow the call to proceed.

For example, if you want to prevent someone from calling a 1-976 number, enter 1976 as the digits to disable.

ATA- and MCA-equipped stations and bandwidth requirements

Each station equipped with an MCA requires a full 64 Kbps of bandwidth to the host PBX.

For stations equipped with ATA devices, the bandwidth used by calls processed on those stations is as follows:

IF	THEN
G.729 compression is being used and the call is a voice call	the voice call is sent as 8 Kbps to the host PBX.
G.729/Fax or G.711 compression is being used and the call is a fax call	the fax call is sent as 64 Kbps.
the call is a local call	the voice call is not compressed. It is sent as 64 Kbps of data across the ISDN BRI B-channel.

The following table identifies the number of MCAs or ATAs that can be connected to the Remote Office 9150 unit:

IF the Remote Office 9150 unit is connected to	THEN you can connect
a 1-slot MIG RLC (supporting 16 users)	four MCAs or ATAs to the Remote Office 9150 unit.
a 2-slot MIG RLC (supporting 32 users)	seven MCAs or ATAs to the Remote Office 9150 unit.

Notes:

- You can have eight MCAs or ATAs installed if an analog telephone or fax machine is *not* installed.
- The total number of digital telephones and ATAs cannot exceed 32.

MIG RLC port type

The MIG RLC port to which each station with remote call capability is assigned can be configured as one of the following port types on the MIG RLC:

- dedicated port: Each station has sole use of the MIG RLC port to which it is assigned.
- shared (multi-user) port: Up to eight persons can share the same MIG RLC port.

  However, only one person can use the MIG RLC port at any given time. All stations that use this type of port respond to the same DN and have identical phoneset configurations. This port type is especially useful for employees who are working in mutually exclusive shifts.
- dynamic port: This is similar to a multi-user port except that persons who share ports in a dynamic pool are assigned to the next available port in the pool.

  There is no correlation between the station and the port on the MIG RLC. This feature is especially useful in free-seated ACD environments where agents log on to the host PBX using their agent IDs.

These port types are defined on the MIG RLC when assigning a remote user to the MIG RLC port. Your telecom network manager or administrator can tell you which port types apply to your office.

Defining the priority level for each station

The MIG RLC port to which a station is assigned can be defined as a normal priority, high priority, circuit-switched only, or IP only station.

Normal priority

If both the IP and circuit-switched networks are used to route calls, calls to and from the station are routed primarily over the IP network. Calls transition between the IP and circuit-switched networks whenever voice Quality of Service levels change. (The voice Quality of Service levels are defined on the Quality of Service screen on the MIG RLC for your Remote Office 9150 unit.)

High priority

If both the IP and circuit-switched networks are used to route calls, calls to and from the station are routed primarily over the IP network. Calls transition between the IP and circuit-switched networks whenever voice Quality of Service levels change. (The voice Quality of Service levels are defined on the Quality of Service screen on the MIG RLC for your Remote Office 9150 unit.)

When the priority reserved setting is also defined on the connection between the MIG RLC and the Remote Office 9150 unit, the following benefits are provided:

- If allowed to use the IP network to process calls (this is transparent to the user), an active call on that station is always one of the first to be transitioned to PSTN trunks when Voice over IP Quality of Service has degraded. (This transition is accomplished using the QoS transitioning technology.)
- Call blocking is reduced because bandwidth is always available to these stations.

  Note: If the reserved bandwidth is being used by other high priority stations, then new calls are processed using unreserved bandwidth.

Note: The number of stations that can be configured on the MIG RLC as high priority depends on the amount of available bandwidth. Ensure that enough bandwidth is available to process calls on normal priority stations.

IP only

Calls to and from the station are routed over the IP network only (if the IP network is used to route calls). QoS transitioning is not available for stations that are defined as IP only.

Circuit only

Calls to and from the station are routed over the circuit-switched network only (if the circuit-switched network is used to route calls). Circuit only stations never experience voice Quality of Service degradation.

Defining the station priority

Station priority configuration consists of the following tasks:

- Select the priority level when configuring the port on the MIG RLC.

  For instructions on defining a MIG RLC port, refer to "Configuring ports" in the *Meridian Internet Gateway Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

- Define the amount of priority reserved bandwidth that high priority stations are allowed to use on the MIG RLC.

  The priority reserved bandwidth is defined for each Remote Office 9150 unit connection. Therefore, all high priority stations at the same site receive the same amount of priority reserved bandwidth, when needed.

  For instructions on configuring priority reserved bandwidth, refer to "Configuring remote site settings" in the *Meridian Internet Gateway Reach Line Card Installation and Administration Guide* (NTP 555-8421-210).

Note: If you are not authorized to modify the configuration on the MIG RLC to which your Remote Office 9150 unit is connected, then contact your MIG RLC network manager or administrator.

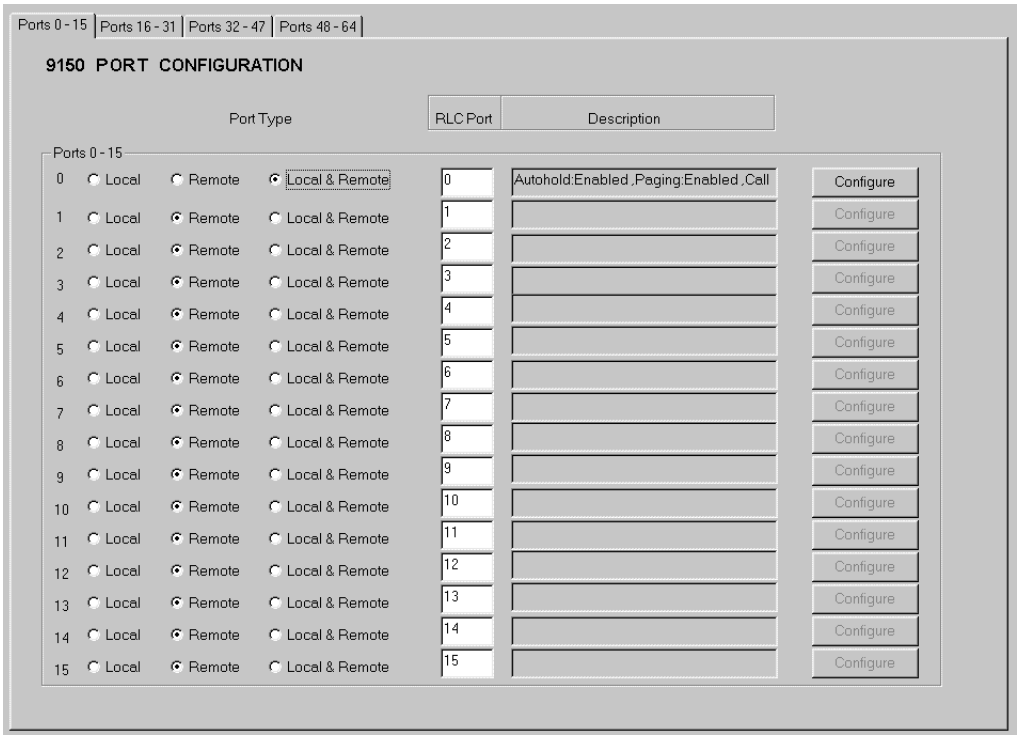
Defining stations

Introduction

To make and receive calls, you must use Configuration to configure each station (telephone or other device such as a fax machine) in your office.

Getting there 9150 → Configuration Manager→ 9150 Port Configuration

9150 Port Configuration sheet



To configure stations

1 Locate the port that you want to configure by clicking the appropriate port range tab, and then scrolling down the list.

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

Ports	Can be assigned to
0–15 and 32–47	digital telephones. **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. **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.

Note: You can use ports 32–47 and 48–63 only if this Remote Office 9150 unit connects to a 2-slot MIG RLC on the host PBX.

2 Under Port Type, click the call processing capability that this station should have:

- Local: if only calls through the local PSTN are allowed. This option enables the Configure button for this port.
- Remote: if only calls through the host PBX are allowed.
- Local and Remote: if both local and remote calls and local station-to-station calling are allowed. This option enables the Configure button for this port so you can configure local station features and keys.

3 Accept the default RLC Port to which this station is assigned, or enter a new RLC port number.

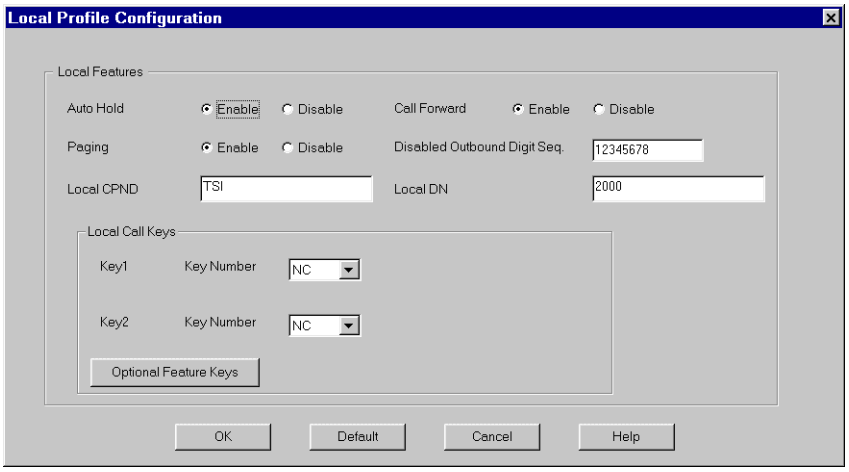
Exception: Do not associate a local-only port with a MIG RLC port.

Notes:

- Generally, the Remote Office 9150 port and MIG RLC port should match to simplify configuration and administration.
- If the station is equipped with an MCA or ATA for data transmission, or if the port is used for fax, the MIG RLC port must be configured on the host PBX with data capability.

4 If you selected Local or Local & Remote, click Configure for the port you are configuring.

Result: The Local Profile Configuration dialog box appears.



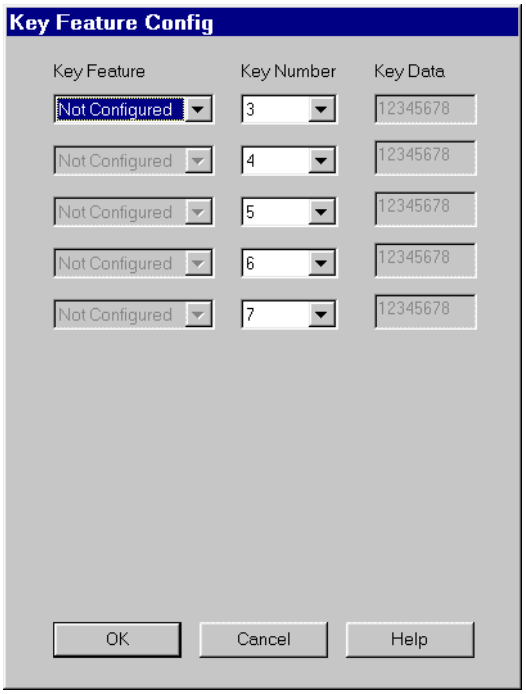
5 Complete the fields as described in “Local Profile Configuration field descriptions” on page 263.

6 Once you have completed the Local Profile Configuration, click OK.

Result: The 9150 Device Configuration sheet reappears. The configurations you set are displayed in the port’s Description box.

Local Profile Configuration field descriptions

Field	Description
Auto Hold	Select Enable if active calls should be automatically put on hold when another call appearance key is pressed. Select Disable if active calls should be disconnected when another call appearance key is pressed.
Call Forward	Select Enable if calls received when a call is already in progress or is not answered should be forwarded to another extension. Select Disable if calls should not be forwarded.
Paging	Select Enable if this station will be allowed to announce pages. Select Disable if this station will not be allowed to announce pages.
Disabled Outbound Digit Seq.	If you want to prevent this station from making a certain type of call, then enter the digits that normally allow that type of call to proceed. **Example:** Enter 1976 to prevent calls to 1-976 numbers. **Note:** You can configure only one digit sequence. In order for calls to be restricted, the dialed number must contain a matching string at the beginning of the number.
Local CPND	Enter the calling party name display for the user to which the station is assigned.
Local DN	Enter the user's local extension number. **Note:** If Auto DN Discovery is enabled on the MIG RLC, then this field is configured to be the same DN as the primary DN configured on the host PBX for this station.

Field	Description
Local Call Keys (Key 1 and Key 2)	The key number identifies the feature key position on the telephone. Select the feature key you want to use for each local call appearance key. **Note:** If the port is configured as local and remote, Key 0 is not recommended. Keys 8 and 9 are recommended. You can select Key 0 if the port is configured as local only. Valid options: 0 through 15
Optional Feature Keys	If you configured the port as Local, click this button to assign local features to specific keys. **Result:** The Key Feature Config dialog box appears. 

Field	Description
Optional Feature Keys (continued)	■ Key Feature Select the name of the feature you want to configure on this key. Valid options: Call Transfer, Call Forward, Auto Dial, Make Set Busy, Not Configured ■ Key Number: The key number identifies the feature key position on the telephone. Select the key you want for the feature you are configuring. **Note:** If the station is configured as local and remote, the key number selected for the feature must match the feature key position defined in the PBX voice port configuration. Valid options: 0 through 15 ■ Key Data Enter the DN to be used by the feature, if applicable.

Defining a fax station

Introduction

The Remote Office 9150 unit provides the ability to connect and use a fax machine. You can define port 64 as the fax machine on the Remote Office 9150 unit in one of the following ways:

TO allow all fax calls to be made or received through	THEN
the local PSTN only	define the fax machine as a local device.
the host PBX	define the fax machine as a remote device.
both the local PSTN and the host PBX	define the fax machine as a local and remote device.

Note: When faxes are sent and received through the host PBX, they are sent uncompressed (that is, they require 64 Kbps of bandwidth).

For instructions on configuring the fax port, see “To configure the fax port” on page 267.

For instructions on configuring a trunk group that rings only on the fax machine, see “To configure trunk groups” on page 247.

Getting there 9150 → Configuration Manager → RLC Port Configuration

9150 Port Configuration sheet

To configure the fax port

1. Locate port 64.
2. On port 64, under Port Type, click the call processing capability the fax machine should have:
   - Local: if only faxes through the local PSTN are allowed. This option enables the Configure button for this port.
   - Remote: if only faxes through the host PBX are allowed.
   - Local and Remote: if both local and remote faxing are allowed. This option enables the Configure button for this port so you can configure local station features and keys.

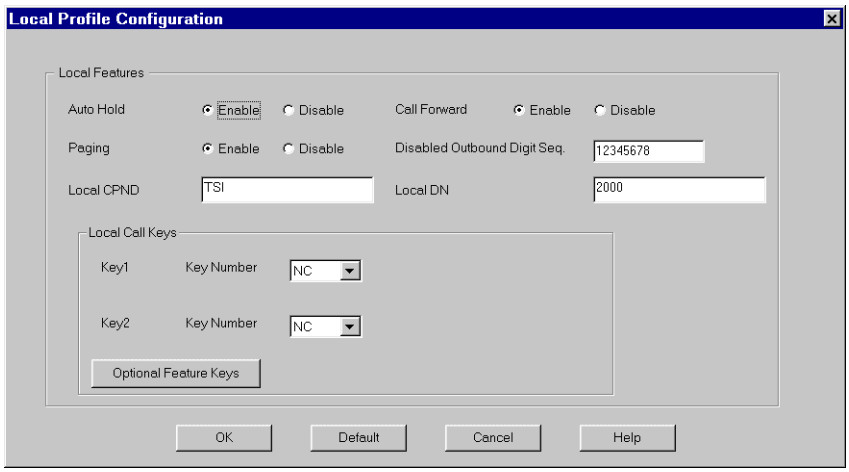
3 Accept the default RLC Port to which this station is assigned, or enter a new RLC port number.

Notes:

- Generally, the Remote Office 9150 port and MIG RLC port should match to simplify configuration and administration.
- For fax transmissions, the MIG RLC port must be configured on the host PBX with data capability.

4 If you selected Local or Local & Remote, click Configure for the port you are configuring.

Result: The Local Profile Configuration dialog box appears.



5 Click Disable under Local Features for the following:

- Auto Hold
- Call Forward
- Paging

6 If applicable, enter the digits that prevent a certain type of call from proceeding in the Disabled Outbound Digit Seq. box.

7 In the Local CPND box, enter a description (for example, FAX).

8 Enter the number used to ring the fax machine in the DN box.

9 Specify the positions of the Local Call Keys.

Note: Key 0 is not recommended for ports defined as local and remote. Keys 8 and 9 are recommended. You can select Key 0 if the port is configured as local only.

10 Click OK to save the information in the temporary work file.

11 To update the Remote Office 9150 unit with the new information, click Send.

IF you are	THEN
logged on to the Remote Office 9150 unit	the changes are written into the Remote Office 9150 unit's buffer. To save the changes in flash memory, choose Upload/Download → Save to Flash.
not logged on to the Remote Office 9150 unit	the following dialog box appears:  Do one of the following: ■ Log on to the Remote Office 9150 unit, and then click Send again. ■ Save the changes to a file on your administration PC.

Chapter 6

Using Remote Office 9150 stations

In this chapter

Modes of operation

Introduction

Digital telephones at your Remote Office 9150 site can operate in the following modes:

- host-controlled
- local-controlled
- online to host PBX
- offline from host PBX

Host-controlled mode

Host-controlled mode means that the host PBX controls the following:

- some display messages that appear on your telephone
- indicator updates such as the message waiting indicator
- calls that you receive from or make to someone at the host PBX site

In host-controlled mode, a voice path is established to the host PBX and signaling messages are passed between the host PBX and the Remote Office 9150 unit.

Exception: If Local Switchover is enabled, and the station-to-station call is completed through the host PBX, signaling messages are passed between the host PBX and Remote Office 9150 unit normally. However, the voice path is established by the Remote Office 9150 unit without consuming host connection bandwidth. The host PBX is aware that the call is active and tracks the status of the phoneset.

If the call cannot be completed through the host PBX, you hear a reorder dial tone.

Local-controlled mode

Local-controlled mode means that the Remote Office 9150 unit at your site controls the following:

- calls to other stations at this site
- calls that are made to or received from your community through your local telephone service provider

Relationship between host-controlled and local-controlled modes

Both the host-controlled and local-controlled modes can be used at the same time. When making or receiving calls, the call modes are controlled by the following telephone keys:

- the host call appearance key (also known as the *primary DN* key)
- the local call appearance key (can sometimes be referred to as the *secondary DN* key)

Host call appearance key

The host call appearance key is the main key you use to make and receive calls. For example, if someone from Finance at Head Office calls you, the call rings on this key. Similarly, if you need to call someone in Payroll at Head Office, you make the call on this key.

Local call appearance key

The local call appearance key is the key you use to make and receive local calls. For example, if your office is working overtime and everyone wants pizza, you call the pizza delivery place on the local call appearance key. Similarly, you use this key if you want to call one of your customers or suppliers or someone else at your site.

Your telephone can have up to two local call appearance keys. Your system administrator can tell you where these keys are and how they are labeled.

Online mode

When in online mode, calls initiated on the host call appearance key are directed through the host PBX. Any long distance charges associated with calls placed through the PBX over the circuit-switched network are charged to the host PBX site. The display on all digital telephones shows “Online Mode.”

Offline mode

When in offline mode, you cannot make calls through the host PBX over either the IP network or circuit-switched network. You can only make calls through your local telephone service provider if your station has been granted local-controlled call capability. The display on all digital telephones show “Offline Mode.”

Why offline mode is important

Your organization is concerned about telephone costs and, as such, wants to ensure that the ISDN BRI line at your site is used for host-controlled calls during business hours only. This is especially important when the ISDN BRI connection between the host PBX and your site is defined as *permanent* (always on) rather than *on demand*. A permanent ISDN BRI connection means the line remains active all the time and incurs charges unless it is put into offline mode.

What controls the online and offline modes

The online and offline modes can be controlled by one or both of the following:

- the online/offline schedule configured for your site on the MIG RLC at the host PBX
- special prefix (SPRE) codes configured on the Remote Office 9150 unit at your site

Online/offline schedule at host PBX

If telephone service costs are an issue, your telecom network administrator defines an online/offline schedule on the MIG RLC port to which your site is assigned. The times at which your site is put into online or offline mode are processed by the host PBX.

For example, if your normal business day is from 9:00 a.m. to 5:00 p.m. from Monday to Friday, the schedule for your site instructs the host PBX to put all stations at your site into online mode during those times. For all other time periods, all stations are in offline mode and, therefore, disconnected from the host PBX.

Note: If you initiate a call on a host call appearance key on any station, then full functionality is allowed even if the time period is outside the automatic offline periods defined on the MIG RLC.

SPRE codes used at your site

If SPRE codes have been defined on the Remote Office 9150 unit at your site, your site can control the times at which stations are put into online or offline modes. You do this by entering one of the following codes on any digital telephone at your site:

- Online SPRE code
- Offline SPRE code

It is recommended that one person at your site be designated as the person responsible for putting the Remote Office 9150 unit (and all stations) into online mode at the beginning of the business day, and into offline mode at the end of the day.

For information about going online or offline, see page 289.

Making and receiving calls

Introduction

The way in which you make outgoing calls depends on which call appearance key you use to make the call.

The call appearance key on which calls are received depends on where the call is coming from.

Receiving incoming calls

The calling line identification (CLID) of an incoming call determines which call appearance key accepts the call.

IF the call	THEN the call
information contains a Called Party Number Display (CPND) that matches a telephone number assigned to one of the ISDN BRI B-channels from your telephone service provider	is routed to the station based on the DNs to Alert configuration on the trunk group to which the B-channel belongs. If the DNs to Alert fields are blank, the call rings on all stations. The call rings on the first local call appearance key on all stations that have been designated to receive calls from this trunk. **Note:** If the first call appearance key is already busy with a call, the call is presented on the second call appearance as a call waiting. The indicator flashes and an alert tone sounds.
comes in on the communication path between the MIG RLC and Remote Office 9150 unit	is routed to the station based on the Remote Office 9150 station to MIG RLC port assignment in the Remote Office 9150 unit's ports configuration. The call rings on the host call appearance key.

IF the call	THEN the call
information contains the DN of another station at this site	rings on the local call appearance key.

Methods for making outgoing calls

You can make an outbound call from a Remote Office 9150 station in one of the following ways.

- Method 1: Pick up the handset.

  This method automatically initiates a host-controlled call.

  Note: If you then press the local call appearance key, the dial tone from the host PBX is changed to local-controlled mode, and the host PBX connection is released.

- Method 2: Press a call appearance key.

  When you press the host call appearance key, a host-controlled call is initiated. When you press the local call appearance key, a local-controlled call is initiated.

To make host-controlled calls

1. Pick up the handset or press the host call appearance key.

   Result: A connection is established with the host PBX and you hear dial tone.

   Note: If a connection to the host PBX cannot be established within a time-out period or no resources are available to carry the call, you hear a reorder dial tone (a fast busy signal), and the following message appears on the telephone display:

   ```
   Release and Try Again
   ```

2. Dial the number of the party you want to call.

   Result: The host PBX receives and processes the dialed digits and rings the called party.

To make outgoing local-controlled calls

Note: You cannot use this procedure to make calls to the host PBX site. If you try, you hear a reorder dial tone (a fast busy signal) and the following message appears on your telephone display:

```
Release and Try Again
```

1 Do one of the following:

IF you are using	THEN
an analog or ATA-equipped station	do the following: **a** Pick up the handset. **Result:** A connection is established with the host PBX and you hear a dial tone. **b** Dial the Local Calling SPRE code. **Result:** The connection is switched to the Remote Office 9150 unit and you hear a dial tone.
a digital telephone	pick up the handset, and then press a local call appearance key. **Result:** A connection is established with the Remote Office 9150 unit and you hear a dial tone.

2 Dial a trunk access code, if required.

Result: The Remote Office 9150 unit obtains a free trunk and you hear another dial tone.

Note: If a trunk is not available, you hear a reorder dial tone (a fast busy signal) and the following message appears on the telephone display:

```
Release and Try Again
```

3 Dial the number of the party you want to call.

Result: Your local telephone service provider receives and processes the dialed digits and rings the called party.

To call another station at your site

Station-to-station calls should be attempted through the host PBX to allow all stations configured as multiple appearance DNs (MADNs) to ring and provide access to voice mail if the call is not answered.

If a connection cannot be established through the host PBX, then you can use the local call appearance key to make the station-to-station call.

1 Pick up the handset or press the host call appearance key.

Result: A connection is established with the Remote Office 9150 unit and you hear a dial tone. The indicator beside the host call appearance key lights.

2 Dial the extension of the party you want to call.

Result: The host PBX receives and processes the dialed digits, and rings the station as well as any other stations that include the dialed DN as an MADN appearance.

Note: The MADN stations could be located at another site (such as the host PBX site).

IF the call is answered by	THEN
an MADN station at another site	a voice path to the host PBX is established and the call proceeds.
a station at this site	all signaling continues to be processed by the host PBX. However, the actual voice path is connected between the two stations and the Remote Office 9150 unit. No trunk bandwidth back to the host PBX is used for the voice path. Trunk bandwidth previously reserved for the call is released and made available to other calls.

Indicator updates

Introduction

Digital telephone indicators reflect the current status of the telephone. For example, they identify when calls are waiting, active, or on hold, or, if your office has voice mail, that messages have been received.

Indicators are updated as follows:

- by the host PBX when a connection between the host PBX and Remote Office 9150 unit is active
- by the Remote Office 9150 unit for feature keys defined on stations with local call capability

Host-controlled indicator updates

Indicators for host-controlled features are updated automatically by the host PBX each time

- an incoming call is received by your site from the host PBX
- an outgoing call is made from your site through the host PBX
- a message waiting indicator (MWI) update is received by someone at your site

Note: If the circuit-switched network is being used and the Remote Office 9150 unit is configured with a permanent (always on) connection to the host PBX, the ISDN BRI service is active and telephone indicators are always updated.

If the IP network is being used to route calls, indicators are always updated.

Local-controlled indicator updates

The following indicators are updated by the Remote Office 9150 unit (that is, these indicator updates are local-controlled):

- host and local call appearance key indicators

  The indicator lights when the handset is taken off-hook, or when you press the call appearance key to go off-hook.

  Note: The Remote Office 9150 unit passes key presses and the on- or off-hook status for the host call appearance key to the host PBX.
- Handsfree
- Mute

Display messages

Introduction

This section describes the messages that can appear on your digital telephone display.

Message descriptions

Message	Description
Going Offline in 30 Secs Going Offline in 20 Secs Going Offline in 10 Secs	This message warns you that all digital telephones at this site are about to go offline in the number of seconds indicated. If any calls are active, they are disconnected when the offline mode is activated. To override, enter the Online SPRE code.
Hostless Mode	The connection to the host PBX cannot be established. The host PBX might be temporarily unavailable. You can still make local calls by using one of the local call appearance keys. **Note:** If Hostless Mode persists, contact your system administrator.
Logged In	If this message appears on your station, then your station is associated with a multi-user or dynamic pool port on the MIG RLC, and it is in logged on status. **Note:** This message appears for approximately ten seconds.

Message	Description
Offline Mode	You cannot make calls through the host PBX over either the IP network or the circuit-switched network. **Note:** If you need to make a call through the host PBX while in offline mode, press the host call appearance key. This establishes a connection to the host PBX and puts all digital telephones at your site into online mode.
Online Mode	You can make and receive calls through the host PBX.
Port Already in Use	If this message appears on your station, then your station is associated with a multi-user or dynamic pool port on the MIG RLC. This message appears if the port to which you are attempting to log on is already being used by someone else.
Port Not Logged In	If this message appears on your station, then your station is associated with a multi-user or dynamic pool port on the MIG RLC, but it is in logged off status.
QoS Recovery	The QoS has returned to normal on the IP network and your active call is being automatically moved to the IP network.
QoS Transition	The QoS has degraded on the IP network and your active call is being automatically moved to the circuit-switched network.
Release and Try Again	All Remote Office 9150 trunks are busy or there are not enough DSP resources to process the call. Try again at a later time. **Note:** Ensure the call you are making is initiated from the appropriate call appearance key: ■ host call appearance key: to call someone at the host PBX site ■ local call appearance key: to make a local PSTN call or to call another station at your site

Message	Description
Resource Limit (1)	If you see this message and hear a fast busy signal when you attempt to make a call, then all trunks are busy. Wait a moment, and then try your call again.
Resource Limit (2)	If you see this message and hear a fast busy signal when you attempt to make a call, then Digital Signal Processor (DSP) resources are all busy. Wait a moment, and then try your call again.

Telephone features operation

Introduction

This section describes how to use the following digital telephone features in host- or local-controlled modes:

- emergency service calls
- Hold
- Call Waiting
- Call Transfer
- Conference
- Call Forward
- Paging

Note: The Conference and Call Forward features are supported for host-controlled calls only.

Emergency service calls

The Remote Office 9150 unit allows an emergency number (for example, 911 in North America) to be programmed by your system administrator.

If the circuit-switched network is used to route calls, and someone dials this emergency service number on any station that is connected to the Remote Office 9150 unit, the call is processed by your local telephone service provider.

You can initiate the emergency service call on either the host call appearance (primary DN) key or local call appearance key. You do not have to dial a trunk access code first.

ATTENTION

If only the IP network is being used to route calls, you must use a telephone that is directly connected to the PSTN to make an emergency service call. If you make the call on a station that is connected to the Remote Office 9150 unit, the call is routed through the host PBX, which can in a different city.

Hold

How Hold works in host-controlled mode

When you press Hold on a host-controlled call, the holding party receives the Hold treatment defined on the host PBX. For example, if the host PBX is configured to play music to holding parties, then the holding party hears music.

You can press any available call appearance key to place a new call.

How Hold works in local-controlled mode

Normally, you put a call on hold by pressing Hold. However, you can also put a local-controlled call automatically on hold by pressing the other local call appearance key. To use this feature, Auto Hold must be enabled on your station.

If Auto Hold is not enabled, and you press a local call appearance key while a call is active on the other local call appearance key, that call is disconnected.

When you press Hold on a local-controlled call, the holding party hears silence. You can press any available call appearance key to place a new call.

Call Waiting

Since the Remote Office 9150 unit does not use host-controlled indicators and the local-controlled indicators are not defined on the host PBX, there are never any indicator conflicts when a call is presented to the station.

However, since the host PBX is not aware when local-controlled calls are active, the host PBX might try to present a call and ring your station while you are busy with a local-controlled call. The Remote Office 9150 unit always checks the status of your station before ringing it. If your station is busy with a call, the alert tone is sounded instead.

How Call Waiting works in host-controlled mode

If you are busy with a host-controlled call, incoming calls are handled as follows:

- An incoming host-controlled call is directed to the call waiting key by the host PBX.
- An incoming local-controlled call flashes the local call appearance key indicator and sounds the alert tone.

How Call Waiting works in local-controlled mode

If you are busy with a local-controlled call, incoming calls are handled as follows:

- An incoming host-controlled call flashes the host call appearance key and sounds the alert tone.
- An incoming local-controlled or station-to-station call flashes the next available local call appearance key and sounds the alert tone. If both local call appearance keys are busy, then the call is not presented to your station.

Call Transfer

Call transfer works the same way in both host- and local-controlled modes. The only difference is the treatment the holding party receives, depending on whether the original call is a host-controlled or local-controlled call.

A call on the host call appearance key can be transferred

- to another station that has remote call capability at this site
- to a station at the host PBX site

A call on the local call appearance key can only be transferred to another station at this site. You cannot transfer a call on the local call appearance key to a station at the host PBX site.

For both, you can do an announced or unannounced (blind) transfer.

To transfer a call

1 Press the Transfer key.

Result: The active call is placed on hold and you hear a dial tone.

2 Dial the number to which you want to transfer the call.

3 Press the Transfer key again to complete the transfer.

Note: You can press the Transfer key while the call is still ringing, or after the called party answers.

Conference

The Conference feature is supported for host-controlled calls only. You cannot conference in someone who must be called through the local PSTN.

To make a conference call

1 Press the Conference key.

Result: The active call is placed on hold and you hear a dial tone.

2 Dial the number of the party you want to conference in.

3 When the called party answers, press the Conference key again to complete the conference.

Call Forward

Call Forward is supported for host-controlled calls only. Your station might be programmed to forward all calls, forward calls when your station is busy, or forward calls when you do not answer.

Paging

When you press a local call appearance key, and then dial the Paging SPRE code, you can announce a page to all other stations at your site.

Note: You can disable Paging for any station.

Going online and offline

Introduction

Stations at the Remote Office 9150 site operate in either online mode or offline mode. This is controlled by one or both of the following:

- SPRE codes to manually toggle all stations at your site between online and offline modes
- an online/offline schedule on the host PBX to automatically toggle all stations at your site between online and offline modes

For a description of the online and offline modes, see “Modes of operation” on page 272.

To use the SPRE code to put all stations into online mode

1. Lift the digital telephone handset, or press one of the local call appearance keys.
2. Dial the pound key (# in North America) followed by the Online SPRE code.

   Note: To learn this code, consult with your system administrator.

   Result: The connection to the host PBX is initiated and negotiated with the host PBX. During this negotiation period (up to 5 seconds), stations at your site cannot be used for host-controlled calls. When negotiation is completed and connection to the host PBX has been established, Online Mode appears on the telephone display.

To use the SPRE code to put all stations into offline mode

1. Lift the digital telephone handset, or press one of the local call appearance keys.
2. Dial the pound key (# in North America) followed by the Offline SPRE code.

   Note: To learn this code, consult with your system administrator.

   Result: Offline Mode appears on the telephone display.

To override an automatic offline event from the host PBX

If the host PBX attempts to process an offline event while you are on a host-controlled call, you are alerted by both an audible alert and a display message indicating that you are about to go offline in 30, 20, or 10 seconds. If you ignore this warning, your call will be disconnected.

To prevent your call from being disconnected, enter the online SPRE code. You can do this without putting your call on hold first. The online SPRE code cancels the offline event, leaving all stations online until the next offline event occurs.

Chapter 7

Administration

In this chapter

Overview

Introduction

This chapter describes the following administration tasks that you perform periodically on the Remote Office 9150 unit:

- Change the administration password.
- Create a configuration backup. If needed, you can use the backup to restore the Remote Office 9150 unit's configuration if it becomes corrupt or lost.
- View statistics and logs.
- Perform firmware and software upgrades.

Administration password

The Remote Office 9150 unit's configuration is protected by two layers of password security. If you want to secure the Remote Office 9150 unit's configuration so that others cannot make configuration changes, you should change the following:

- Configuration Manager password
- Remote Office 9150 unit's password

Backups and restores

Create a backup copy of the Remote Office 9150 unit's configuration by downloading the Remote Office 9150 unit's configuration from flash memory to a text file on your administration PC.

Restore the Remote Office 9150 unit'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.

Statistics and logs

The Remote Office 9150 unit keeps track of system performance through the maintenance of logs. You can use the following procedure to view the information kept in these logs.

The statistics logs help you determine how much traffic is being processed by the Remote Office 9150 unit. By becoming familiar with the traffic patterns, you can determine if network adjustments must be made.

Firmware and software upgrades

There are two types of upgrades that can be performed for your Remote Office 9150 unit:

- a Configuration Manager software upgrade on your PC
- a Remote Office 9150 firmware upgrade

The Configuration Manager software is used to configure or administer the Remote Office 9150 unit. The firmware contains the code necessary for operating the Remote Office 9150 unit.

Changing the administration password

Introduction

The Remote Office 9150 unit's configuration is protected by two layers of password security. If you want to secure the Remote Office 9150 unit's configuration so that others cannot make configuration changes, you should change the following:

- the Configuration Manager password

  This password prevents unauthorized offline configuration changes from being performed.

- the Remote Office 9150 unit's password

  This password prevents unauthorized online changes of the configuration residing in the Remote Office 9150 unit's flash memory.

ATTENTION

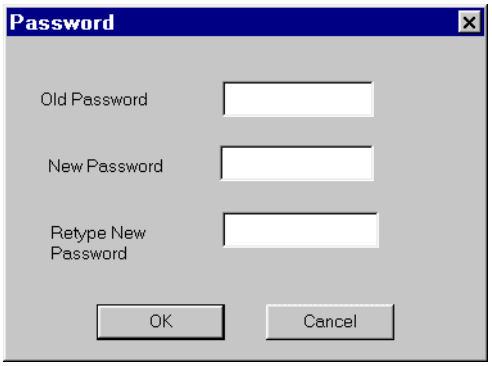
Ensure that you record the passwords and store them in a safe, secure place. If you forget or lose the password, you must contact your Nortel Networks technical support representative.

Getting there 9150 → Configuration Manager

To change the Configuration Manager password

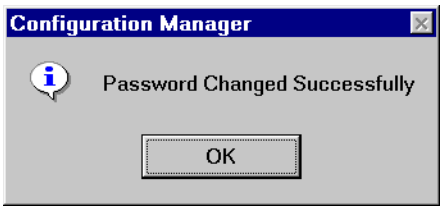
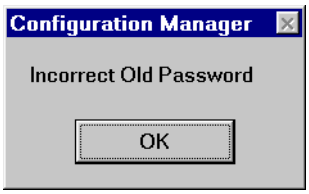
1 From the menu, choose Connect → Change Password → Local.

Result: The Change Password dialog box appears.



2 Complete the fields as described in “Password dialog box field descriptions” on page 298.

3 Click OK.

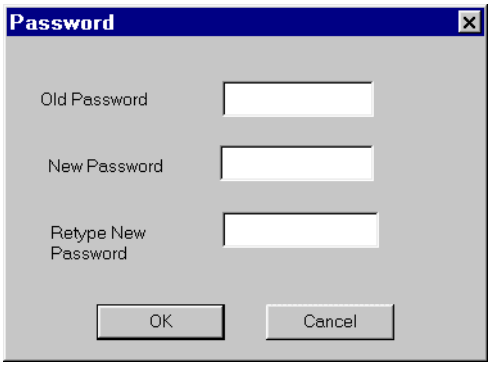
IF the password change	THEN
was successful	the following appears:  Click OK.
was not successful	one of the following messages appears: 

IF the password change	THEN
was not successful (continued)	 Click OK, and then try again.

To change the Remote Office 9150 unit's password

1 From the menu, choose Connect → Change Password → Board.

Result: The Password dialog box appears.



2 Complete the fields as described in "Password dialog box field descriptions" on page 298.

3 Click OK.

IF the password change	THEN
was successful	the following appears:  **Note:** This means the password has been written to the Remote Office 9150 unit's flash memory. Click OK.
was not successful	one of the following messages appears:   Click OK, and then try again.

4 From the menu, choose Upload/Download → Save to Flash.

Result: The Remote Office 9150 unit's flash memory is updated with the new password.

5 Restart the Remote Office 9150 unit.

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.

Section A: Performing backups and restores

In this section

Overview

Introduction

This section describes how to create a backup copy of the Remote Office 9150 unit'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 Remote Office 9150 unit's configuration by downloading the Remote Office 9150 unit's configuration from flash memory to a text file on your administration PC.

How restores are done

You restore the Remote Office 9150 unit'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 Remote Office 9150 unit's configuration by downloading the Remote Office 9150 unit'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 Remote Office 9150 unit is an extension of the telecommunications and data network. It is extremely important that you keep a backup copy of the Remote Office 9150 unit's configuration. If the Remote Office 9150 unit'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.

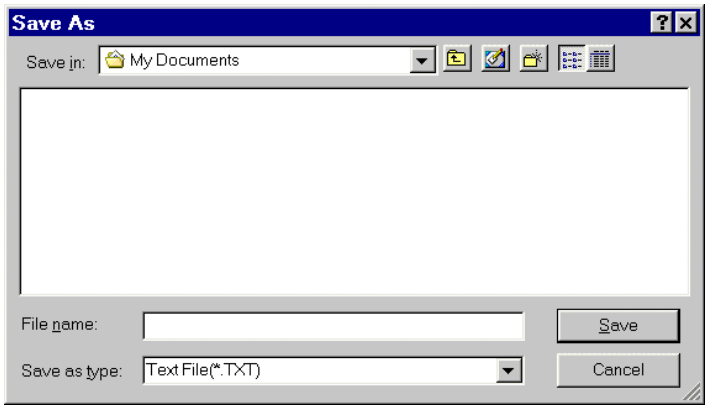
Nortel Networks recommends that you keep the backup files indefinitely.

Getting there 9150 → 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.

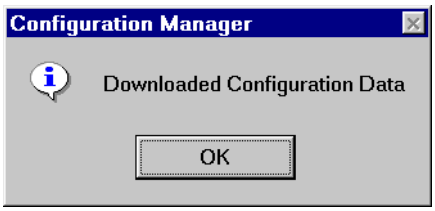
Note: This configuration file will become your backup file, so ensure the file name is meaningful. The file name's extension is .TXT.

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:



5 Click OK.

Restoring the configuration

Introduction

Restore the Remote Office 9150 unit'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 Remote Office 9150 unit, you must do the following:

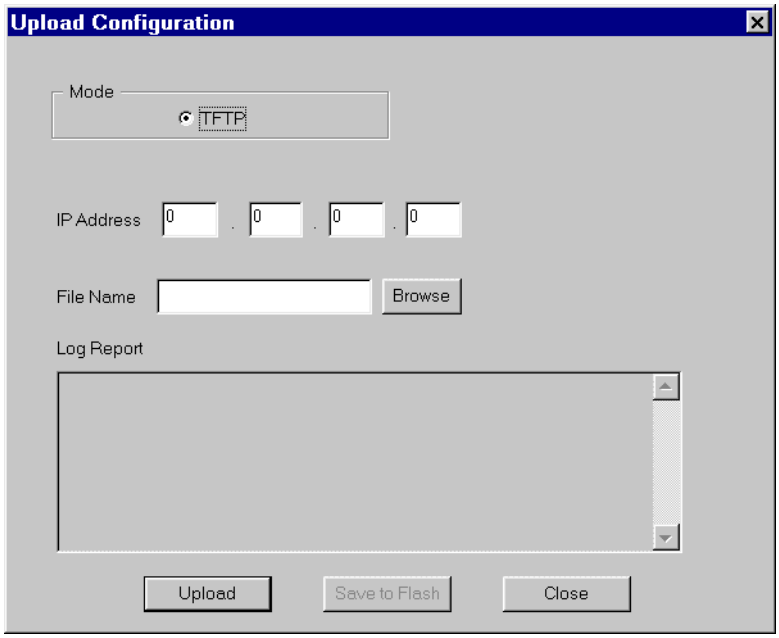
1. Start the TFTP server application.
2. Ensure the TFTP base directory reflects the directory where the configuration file you want to upload is located.

Getting there 9150 → 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.

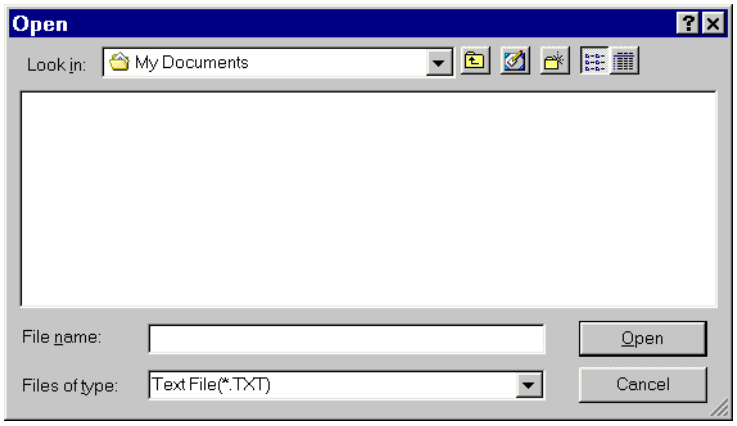


2 In the IP Address boxes, enter the IP address of the TFTP server.

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 configuration file is located.

6 Select the file, and then click Open.

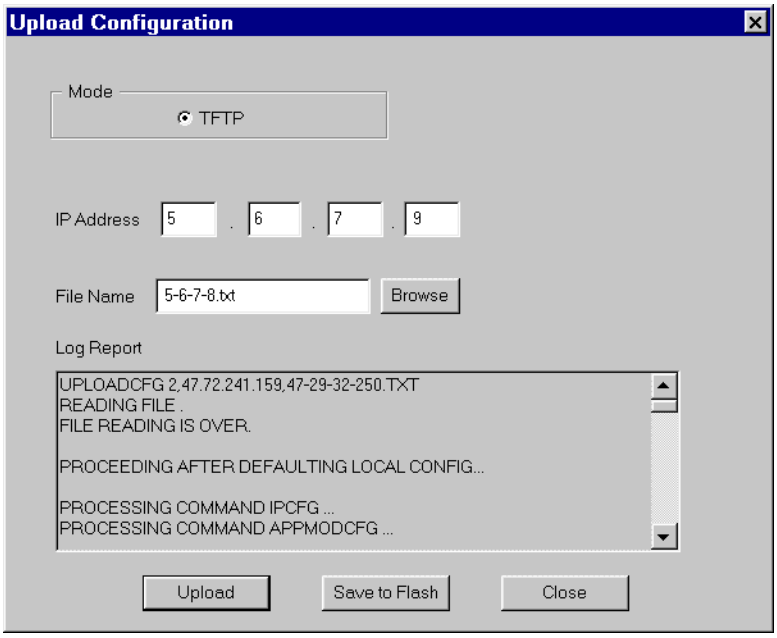
Result: You are returned to the Upload Configuration dialog box. The file you selected is shown in the File Name box.

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.



CAUTION

Risk of incorrect operation due to partial configuration

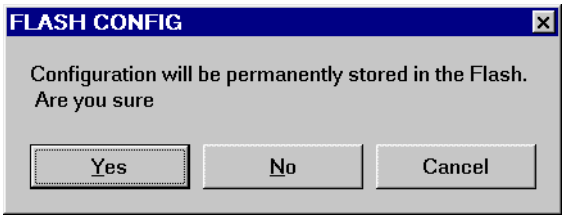
Do not interrupt the configuration upload. If you interrupt the configuration upload, this results in an incomplete configuration in the Remote Office 9150 unit's database.

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.
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:



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 Remote Office 9150 unit.

Note: For instructions, see “Performing a system restart or shutdown” on page 198.

Section B: Working with system logs

In this section

Overview

Introduction

The Remote Office 9150 unit keeps track of system performance through the maintenance of logs. Configuration Manager provides several ways to work with these logs to get the information you need to keep your 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 311 to view that information.

Resizing logs

You might find that you want logs to occupy a larger or smaller percentage of memory on the Remote Office 9150 unit. The procedure described on page 313 allows you to change the size of the logs that the Remote Office 9150 unit maintains.

Clearing logs

The Remote Office 9150 unit allows you to increase memory by clearing the log queue whenever you decide to do so. You can use the procedure described on page 314 to discard information from the logs when it is no longer useful.

Displaying logs

Introduction

The Remote Office 9150 unit keeps track of system performance through the maintenance of logs. Each line stored in the log represents a separate action completed by the unit.

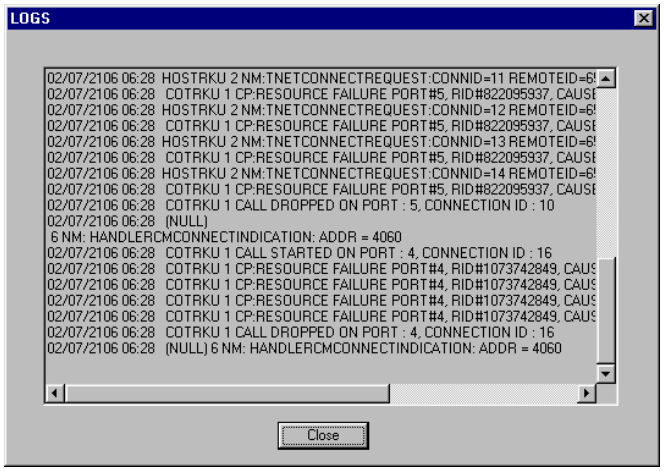
Use these logs when you want to troubleshoot system problems. You can print the log to a text file by copying the information from the log window, and then pasting it into a text file.

Getting there 9150 → Configuration Manager

To display logs

From the menu, choose Alarms/Stats/Logs → Display Logs.

Result: The Remote Office 9150 unit 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.



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.

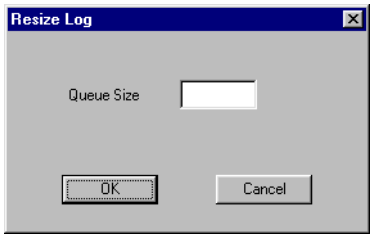
You might find that you want the logs to occupy a larger or smaller percentage of memory on the Remote Office 9150 unit. You can use the following procedure to change the size of the logs that the Remote Office 9150 unit keeps.

Getting there 9150 → Configuration Manager

To change the size of Remote Office 9150 unit logs

1 From the menu, choose Alarms/Stats/Logs → Resize Logs.

Result: The Resize Log dialog box appears.



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

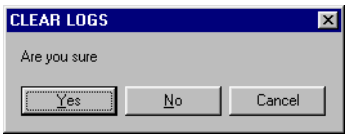
The Remote Office 9150 unit allows you to increase memory by clearing the log queue. Use the following procedure to discard information from the logs that is no longer useful.

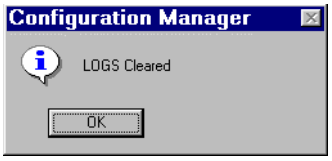
Getting there 9150 → Configuration Manager

To clear logs

1 From the menu, choose Alarms/Stats/Logs → Clear Logs.

Result: The CLEAR LOGS dialog box appears.



IF you select	THEN
No or Cancel	the dialog box closes and the logs remain as is.
Yes	the Remote Office 9150 logs are cleared and the following confirmation dialog box appears:  Click OK.

Section C: Viewing statistics

In this section

Overview

Introduction

This section describes the statistics logs that you can view in Configuration Manager. These statistics logs help you determine how much traffic is being processed by the Remote Office 9150 unit. By becoming familiar with the traffic patterns, you can determine if network adjustments must be made.

Trunk Connection Statistics

The Trunk Connection Statistics log allows you to see how much traffic is being processed over each B-channel. Use this statistics log to determine which trunks get used the most.

Bandwidth Connection Statistics

The Bandwidth Connection Statistics log allows you to see how much bandwidth the Remote Office 9150 unit can use, and how much is actually being used. Use this statistics log to help you determine if you need to add more bandwidth on circuit-switched network or IP connections.

Caller Information Statistics

The Caller Information Statistics log 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 the stability of voice Quality of Service on your IP network.

Hardware Statistics

The Hardware Statistics log is a listing of what modules you have installed in your Remote Office 9150 unit. Use it to determine which module positions in the Remote Office 9150 unit are populated, and what they contain.

Local Call Statistics

The Local Call Statistics log allows you to see how many local calls were processed by the Remote Office 9150 unit, and how long they lasted. Use this statistics log to determine how much traffic is being processed through the local PSTN.

Remote Call Statistics

The Remote Call Statistics log allows you to see how many calls were processed by the Remote Office 9150 unit through the host PBX, and how long they lasted. Use this statistics log to determine how much traffic is being processed through the host PBX.

Trunk Connection Statistics screen

Introduction

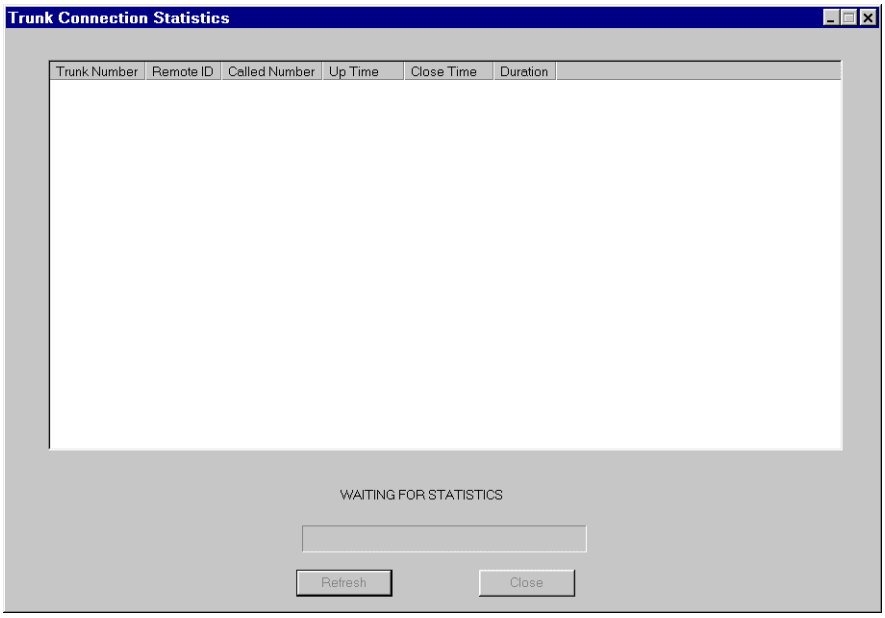
The Trunk Connection Statistics screen allows you to see the amount of traffic that is processed over each B-channel. Use this statistics log to determine which trunks get used the most.

Getting there 9150 → Configuration Manager

To display the trunk connection statistics

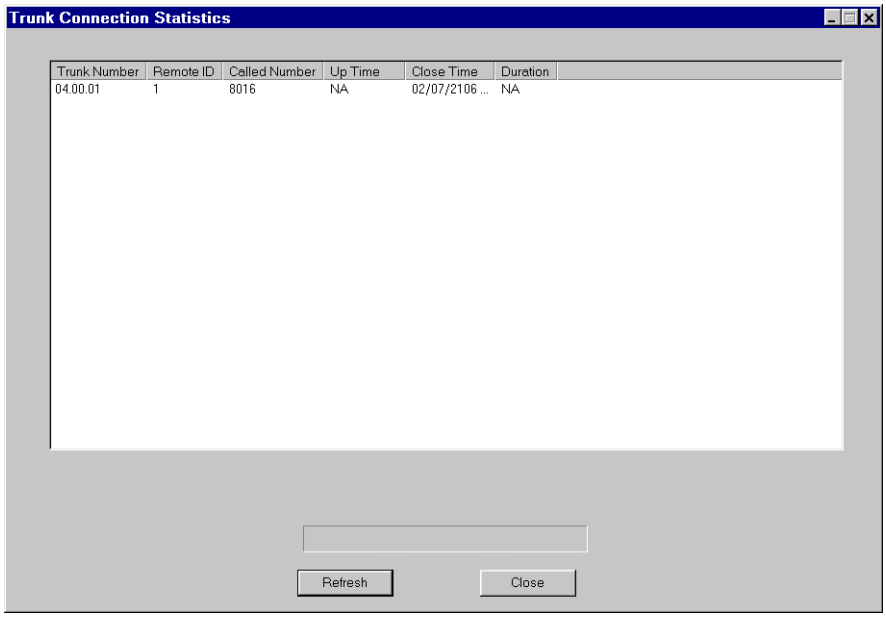
1 From the menu, choose Alarms/Stats/Logs → Trunk Connection Statistics.

Result: The Trunk Connection Statistics screen appears.



2 Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.



3 Do one of the following:

- To refresh the statistics, click Refresh.
- To close the statistics screen, click Close.

Trunk Connection Statistics field descriptions

Column	Description
Trunk Number	Identifies the ISDN BRI module and B-channel used for the call.
Remote ID	Identifies the Remote Office 9150 station (port) that initiated the call.
Called Number	Identifies the telephone number used to initiate the connection.
Up Time	If available, identifies the time at which the call began.

Column	Description
Close Time	Identifies the time at which the call ended.
Duration	Identifies how long the call was active.

Bandwidth Connection Statistics screen

Introduction

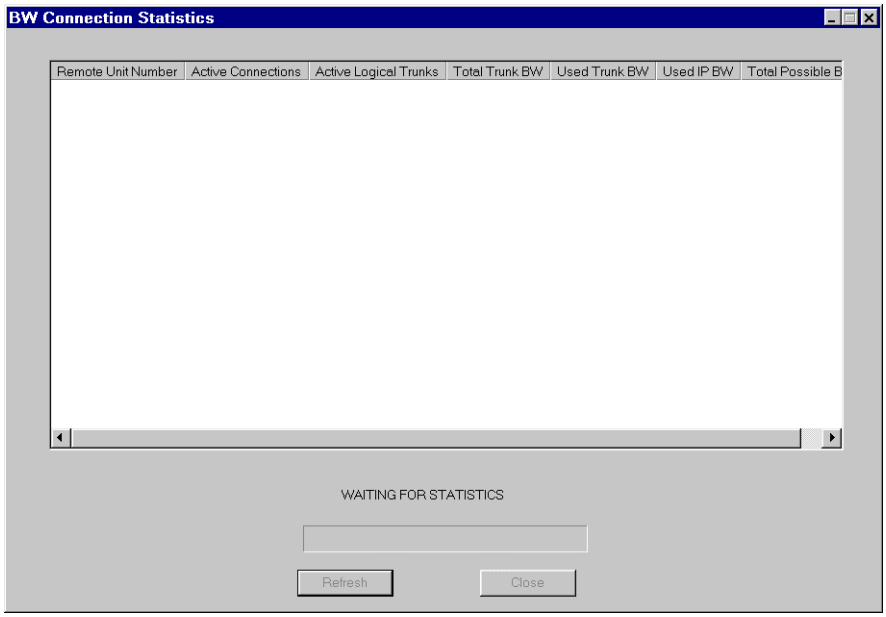
The Bandwidth Connection Statistics screen allows you to see how much bandwidth the Remote Office 9150 unit can use, and how much is actually being used. Use this statistics log to help you determine if you need to add more bandwidth on circuit-switched network or IP connections.

Getting there 9150 → Configuration Manager

To display the bandwidth connection statistics

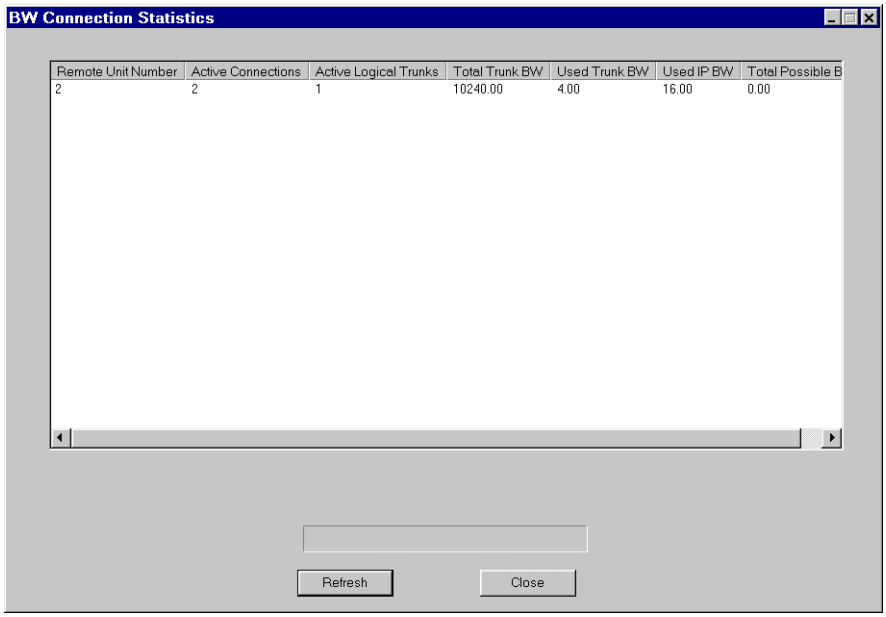
1 From the menu, choose Alarms/Stats/Logs → BW Connection Statistics.

Result: The BW Connection Statistics screen appears.



2 Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.



3 Do one of the following:

- To refresh the statistics, click Refresh.
- To close the statistics screen, click Close.

BW Connection Statistics field descriptions

Column	Description
Remote Unit Number	Identifies the Remote Office 9150 unit's board ID.
Active Connections	Identifies the number of calls in progress.
Active Logical Trunks	Identifies the number of connections that are currently active with the MIG RLC on the host PBX.

Column	Description
Total Trunk BW	Identifies the possible circuit-switched bandwidth available on the Remote Office 9150 unit.
Used Trunk BW	Identifies the amount of circuit-switched bandwidth currently in use.
Used IP BW	Identifies the amount of IP bandwidth currently in use in Kbps.
Total Possible Bandwidth	Identifies the possible combined circuit-switched and IP bandwidth that can be used by the Remote Office 9150 unit.

Caller Information Statistics screen

Introduction

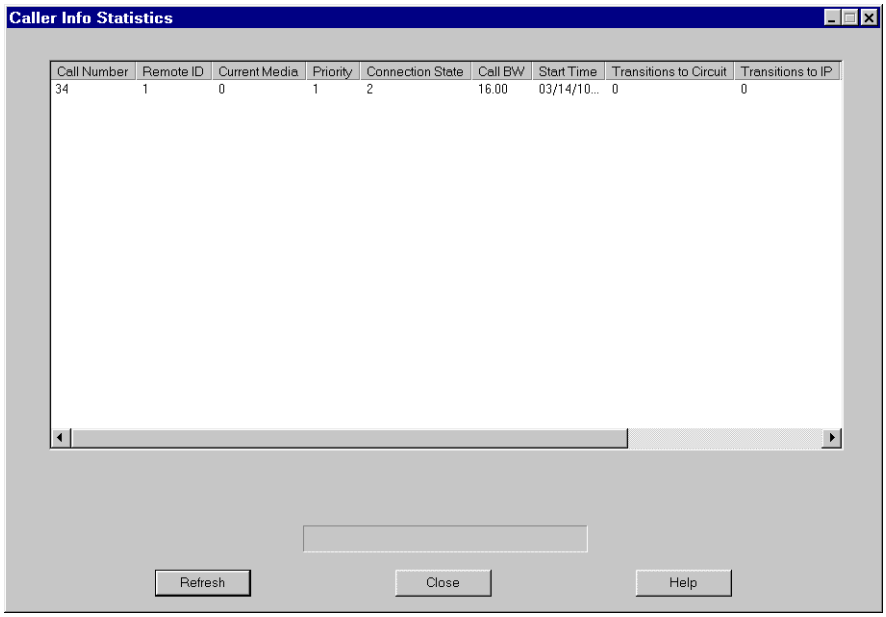
The Caller Information Statistics screen allows you to see the types of calls being made (IP or circuit-switched), and how often QoS transitions occur. Use this statistics log to help you determine if the voice Quality of Service on your IP network is stable.

Getting there 9150 → Configuration Manager

To display the caller information statistics

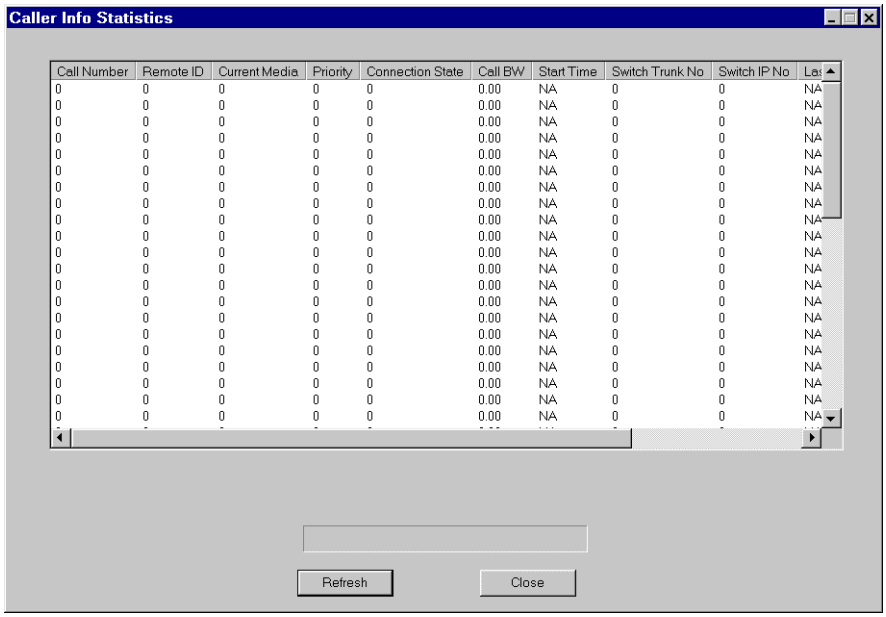
1 From the menu, choose Alarms/Stats/Logs → Caller Info Statistics.

Result: The Caller Info Statistics screen appears.



2 Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.



3 Do one of the following:

- To refresh the statistics, click Refresh.
- To close the statistics screen, click Close.

Caller Info Statistics field descriptions

Column	Description
Call Number	Identifies the number of the call that was processed by the Remote Office 9150 unit.
Remote ID	Identifies the board ID of the remote site that was involved in the call.

Column	Description
Current Media	Identifies whether the call was over the IP network or circuit-switched network.
Priority	Identifies the priority that applied to the call (circuit-switched only, IP only, high, or normal).
Connection State	Identifies if the call is currently active or not.
Call BW	Identifies the amount of bandwidth 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 moved from the IP network to the circuit-switched network.
Last Transition to IP	Identifies the last time the call was moved from the circuit-switched network to the IP network.

Hardware Statistics screen

Introduction

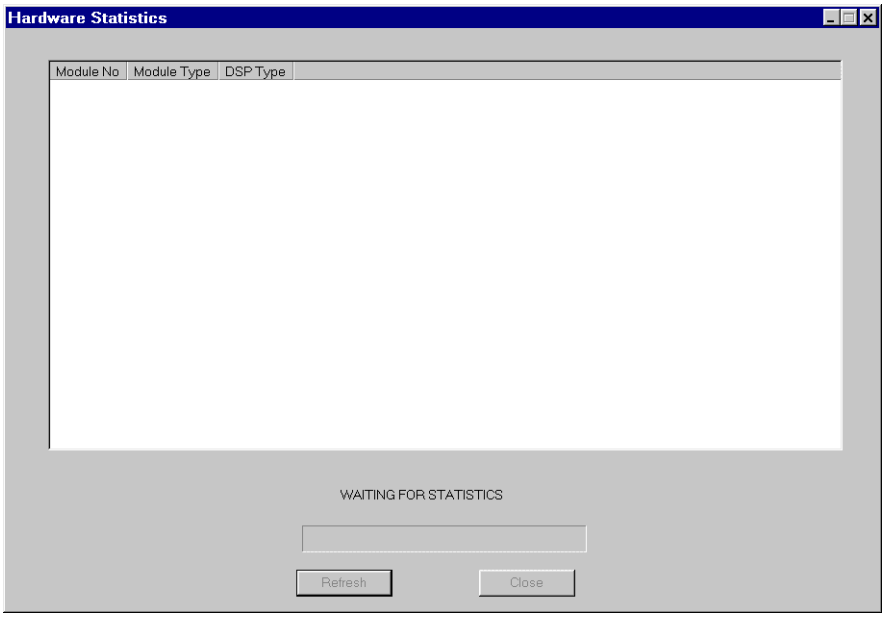
The Hardware Statistics screen provides a listing of what modules you have installed in your Remote Office 9150 unit. Use it to determine which module positions in the Remote Office 9150 unit are populated, and what they contain.

Getting there 9150 → Configuration Manager

To display the hardware statistics

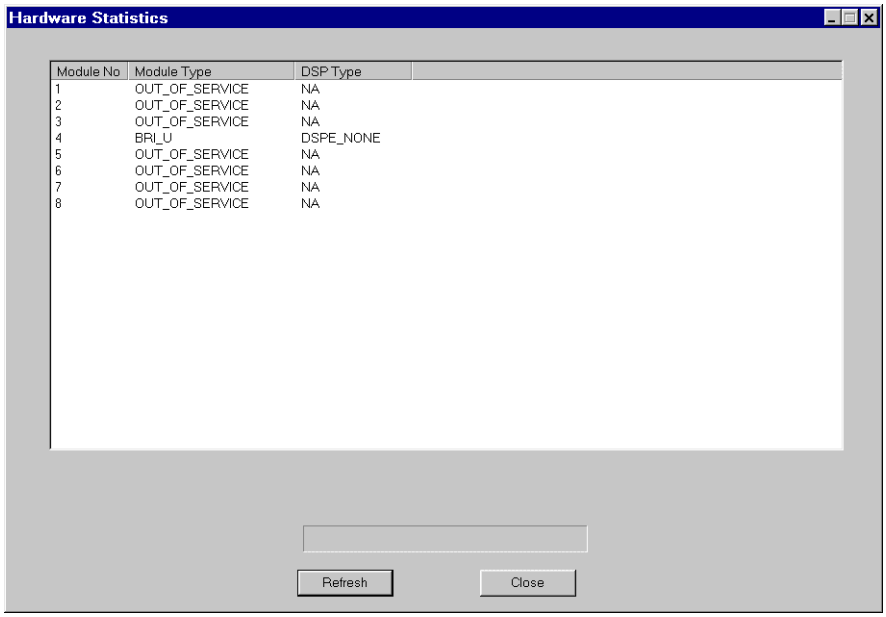
1 From the menu, choose Alarms/Stats/Logs → Hardware Statistics.

Result: The Hardware Statistics screen appears.



2 Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.



3 Do one of the following:

- To refresh the statistics, click Refresh.
- To close the statistics screen, click Close.

Hardware Statistics field descriptions

Column	Description
Module No.	Identifies the module position on the Remote Office 9150 motherboard.
Module Type	Identifies what has been installed in the module position: ■ BRI_U or BRI_ST: An ISDN BRI trunk interface module is installed. ■ DSP: A DSP application module is installed. ■ OUT_OF_SERVICE: No hardware is installed.

Column	Description
DSP Type	Identifies the type of DSP the module contains. **Note:** All ISDN BRI modules should display DSP_NONE.

Local Call Statistics screen

Introduction

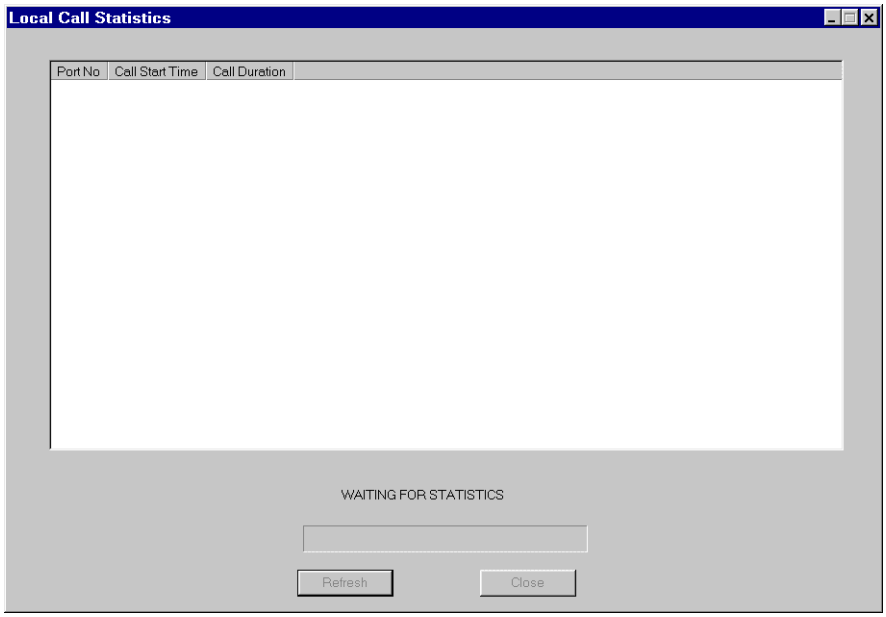
The Local Call Statistics screen allows you to see how many local calls were processed by the Remote Office 9150 unit, and how long they lasted. Use this statistics log to determine how much traffic is being processed through the local PSTN.

Getting there 9150 → Configuration Manager

To display the local call statistics

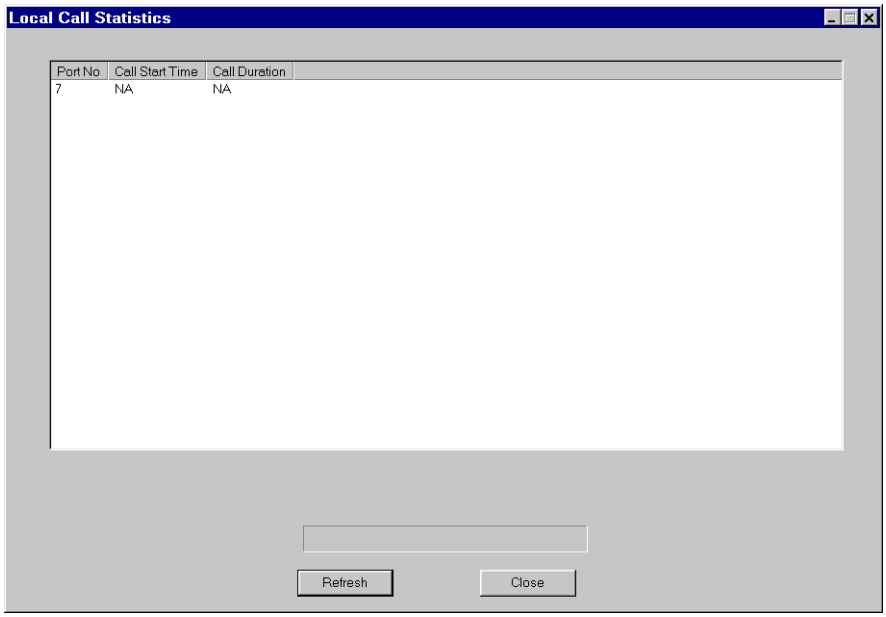
1 From the menu, choose Alarms/Stats/Logs → Local Call Stats.

Result: The Local Call Statistics screen appears.



2 Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.



3 Do one of the following:

- To refresh the statistics, click Refresh.
- To close the statistics screen, click Close.

Local Call Statistics field descriptions

Column	Description
Port No.	Identifies the Remote Office 9150 port through which the call was processed.
Call Start Time	Identifies the time when the call started.
Call Duration	Identifies the length of the call.

Remote Call Statistics screen

Introduction

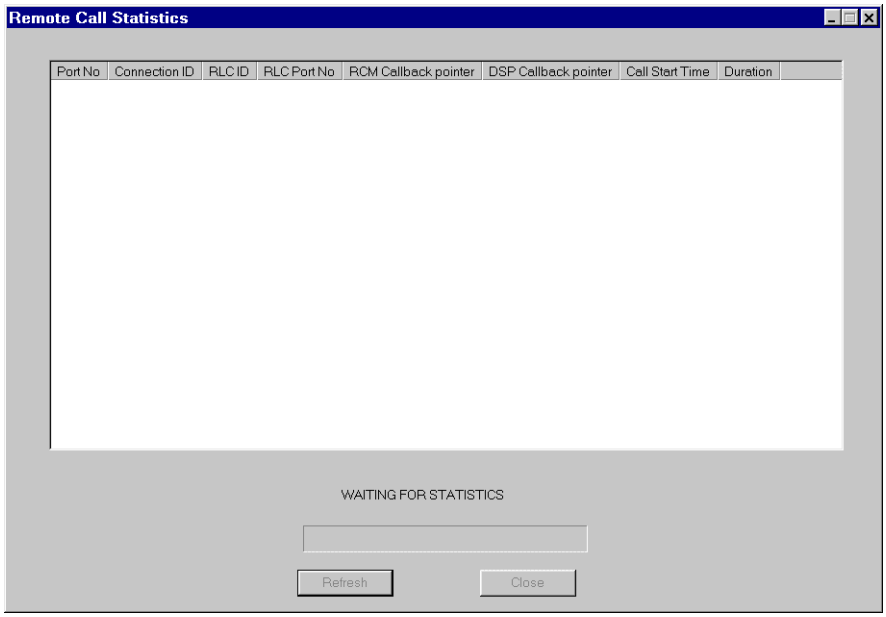
The Remote Call Statistics screen allows you to see how many calls were processed by the Remote Office 9150 unit through the host PBX, and how long they lasted. Use this statistics log to determine how much traffic is being processed through the host PBX.

Getting there 9150 → Configuration Manager

To display the remote call statistics

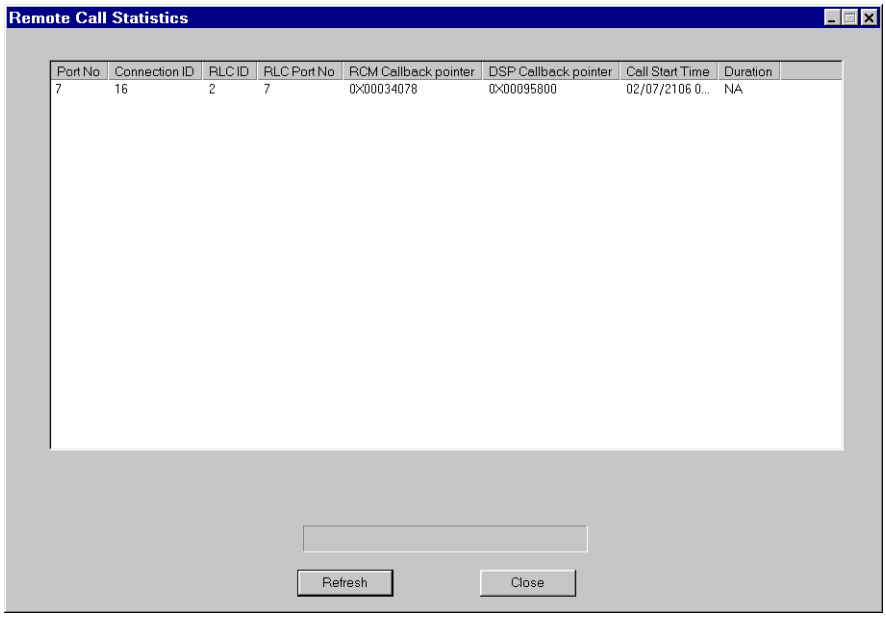
1 From the menu, choose Alarms/Stats/Logs → Remote Call Stats.

Result: The Remote Call Statistics screen appears.



2 Wait while Configuration Manager gathers statistics from the Remote Office 9150 unit's system logs.

Result: The statistics appear. The following is an example.



3 Do one of the following:

- To refresh the statistics, click Refresh.
- To close the statistics screen, click Close.

Remote Call Statistics field descriptions

Column	Description
Port No.	Identifies the Remote Office 9150 port through which the call was processed.
Connection ID	A sequential number used for tracking individual calls.
RLC ID	Identifies the board ID of the MIG RLC that processed the call.

Column	Description
RLC Port No.	Identifies the MIG RLC port that processed the call.
RCM Callback pointer	Identifies the internal program routine used. **Note:** This information is for technical support use only.
DSP Callback pointer	Identifies the internal program routine used. **Note:** This information is for technical support use only.
Call Start Time	Identifies when the call began.
Duration	Identifies how long the call lasted.

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 Remote Office 9150 unit:

- a Configuration Manager software upgrade on your PC
- a Remote Office 9150 firmware upgrade

You use the Configuration Manager software to configure or administer the Remote Office 9150 unit. The firmware contains the code necessary for operating the Remote Office 9150 unit.

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 you upgrade the Remote Office 9150 unit's firmware. This ensures that communication problems between the MIG RLC and Remote Office 9150 unit 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.

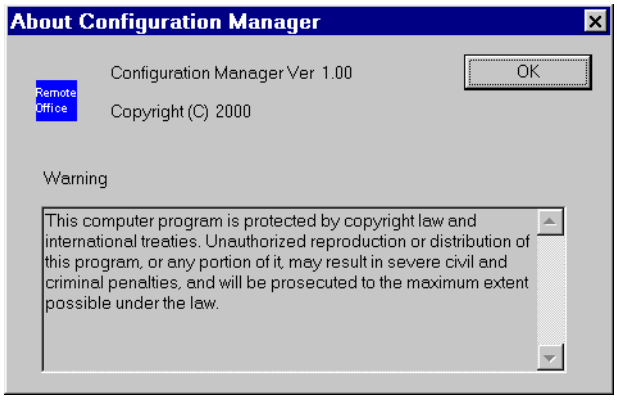
Why verify the firmware and software release

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.

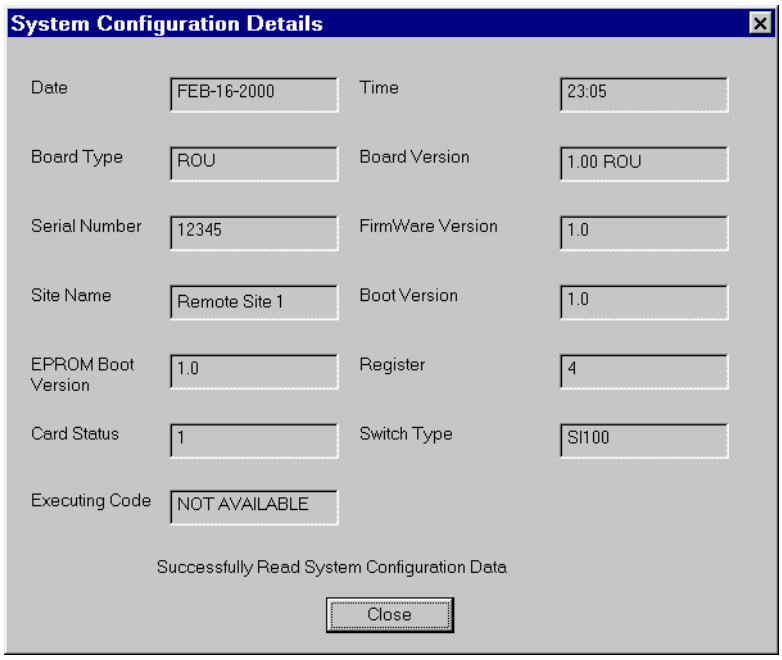
Result: The following dialog box appears:



To verify the firmware version

1 From the menu, choose System Information → System Data.

2 The System Configuration Details screen appears.



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 Remote Office 9150 unit:

- Configuration Manager software upgrade

  You use Configuration Manager software to configure or administer the Remote Office 9150 unit.

- firmware upgrades
  - Remote Office 9150 motherboard firmware

    Note: This includes any firmware updates that have been made for DSP application modules.
  - trunk interface module firmware

  The firmware contains the code necessary for operating the Remote Office 9150 unit.

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 342.

Extracting upgrade files from the download file

Introduction

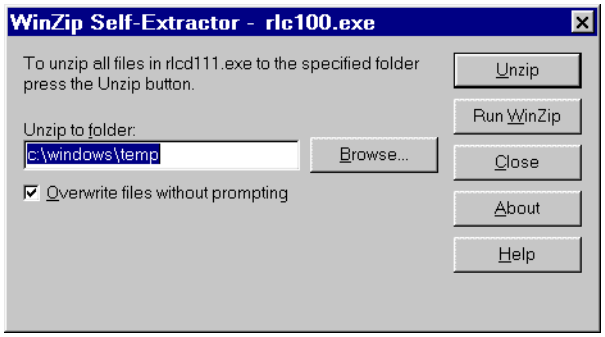
Before you perform an upgrade, ensure you have obtained the latest upgrade files from your Nortel Networks distributor. The upgrade files are enclosed in self-extracting executable files. You must extract the upgrade files before you can perform the upgrade.

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.



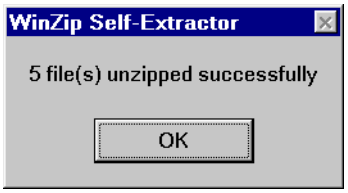
3 Review the information presented and make changes as necessary.

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 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 Remote Office 9150 unit. 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 338.

CAUTION

Risk of incorrect operation

You must ensure that the MIG RLC's firmware has been upgraded before you upgrade the Remote Office 9150 unit's firmware. This ensures that communication problems between the MIG RLC and Remote Office 9150 unit 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, you 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 340.

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 342.

3 Start the TFTP server application.

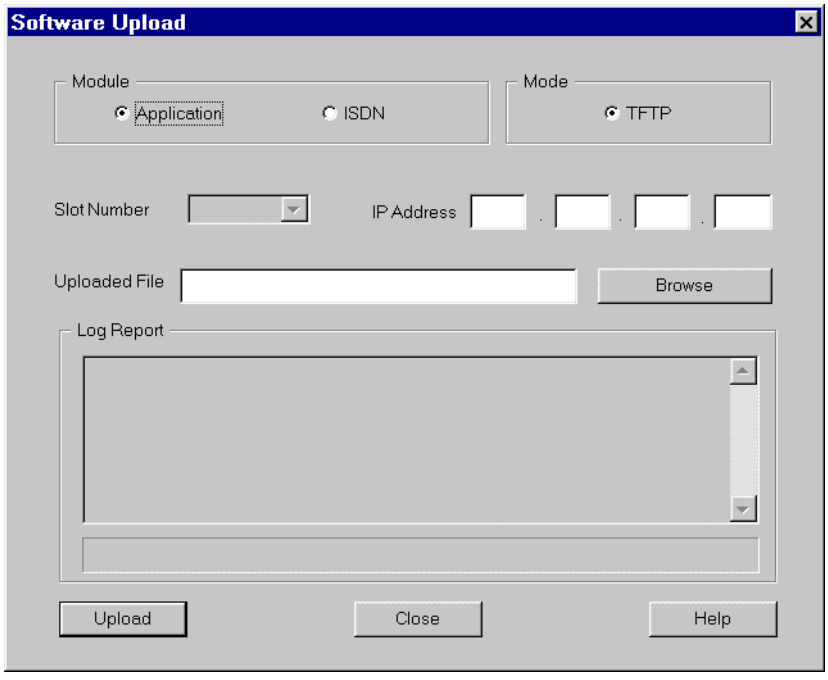
4 Ensure the TFTP base directory reflects the directory where the firmware upgrade file you want to use is located.

Getting there 9150→ Configuration Manager

To upgrade the firmware

1 From the menu, choose Upload/Download → Upload S/W.

Result: The Software Upload screen appears.



2 Do one of the following:

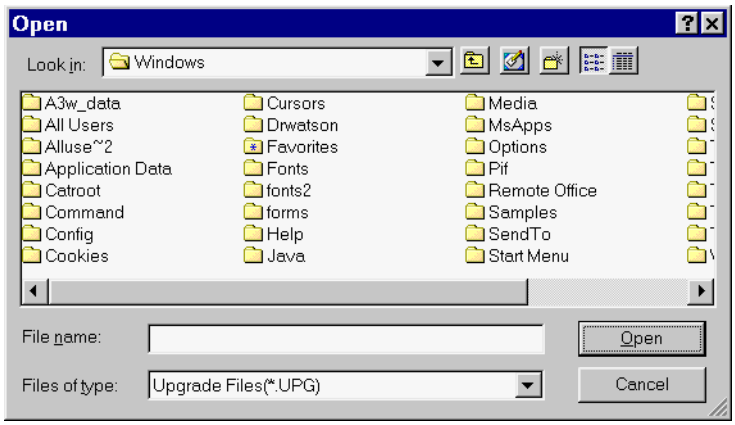
IF you are upgrading	THEN
motherboard firmware	in the Module section, click Application.
ISDN BRI module firmware	do the following: **a** In the Module section, click ISDN. **b** Enter the position on the motherboard where the ISDN BRI module is installed. Valid values: 4 through 7

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.



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.

Examples:

- For motherboard firmware, select 9150-100.upg, and then click Open.
- For ISDN BRI module firmware, select briv15u.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 Remote Office 9150 unit.

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 338.

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

This chapter describes the troubleshooting you can do to resolve any problems you might have.

LEDs

During the Remote Office 9150 unit power-up cycle, watch the front panel of the Remote Office 9150 unit. The LEDs should appear as follows:

- The Power LED should light and remain lit.
- The Status LED stays lit after the power-up cycle is completed. When the Status LED is lit all the time, the unit is healthy.
- The remaining LEDs flash whenever there is network activity.

This chapter describes what to do if LEDs do not display correctly, or when they indicate activity that could be a cause for concern.

Digital telephone

Generally, digital telephones should behave the same as if they were directly connected to a PBX. They receive a dial tone, display messages, and indicator updates. This chapter describes what to do when no dial tone is received, when there is no indicator activity, or when error messages specific to Remote Office 9150 appear.

Device connectivity

If you observe network activity that deviates from normal or baseline activity on the Remote Office 9150 network, or if you have trouble connecting to the Remote Office 9150 unit, this chapter describes what to do.

Software problems

If you have trouble completing a task with Configuration Manager, this chapter describes what to do.

Before you begin

Introduction

If you experience problems in setting up or running your Remote Office 9150 unit, this chapter will help you to isolate and solve the problem.

Identifying why the 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 troubleshooting in the sequence presented in this chapter.
	no	Answer the next question.
Did the Remote Office 9150 unit 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 done correctly. **2** Check the hardware components to ensure they are in working order. **3** Perform troubleshooting for the specific component.
	no	Contact your telecom or data network administrator. There might be a problem with the network.

Remote Office 9150 LEDs

Introduction

During a Remote Office 9150 unit power-up cycle, watch the front panel of the Remote Office 9150 unit. The LEDs should appear as follows:

- The Power LED should light and remain lit.
- The Status LED should stay lit after the power-up cycle is completed. When the Status LED is lit all the time, the unit is healthy.
- 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 Status LED is not lit.	**1** Did the Status LED ever illuminate? If not, contact your Nortel Networks distributor. There might be a hardware problem. **2** Are other LEDs lit or flashing? If no, ensure the power cable is connected to both the power source and the Remote Office 9150 unit. If it has become disconnected, reconnect it. **3** If the Status LED is still out, contact your Nortel Networks distributor. There might be a hardware problem.
No LEDs are lit on the Remote Office 9150 unit.	**1** Ensure that the Remote Office 9150 unit is connected to a power source. **2** If you are using an uninterruptible power supply (UPS), ensure the UPS is powered on. **3** Verify that the AC power source is operational.

Symptom	What to do
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 Remote Office 9150 unit 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.

Digital telephone

Introduction

This section identifies some problems that could occur on the digital telephone, and describes what to do to resolve them.

Symptom descriptions

If you are having trouble with digital telephones, perform troubleshooting as described in the following table:

Symptom	What to do
There is no dial tone when pressing either the host call appearance or local call appearance keys.	**1** Is this a first-time installation? If yes, perform troubleshooting as described in “What to do if the telephone connection tests do not work” on page 157. **2** If you are trying to make a host-controlled call, check the IP network and ensure that ■ it is not down ■ traffic is being routed between the Remote Office 9150 unit and MIG RLC on the host PBX **3** If you are trying to make a host- or local-controlled call, Ensure the ISDN BRI line is working. Ask your service provider to check this. **4** Restart the MIG RLC, wait one minute, and then restart the Remote Office 9150 unit. **5** Ensure the MIG RLC is enabled in its host PBX slot. In Load 97 on the Meridian 1 PBX, stat the MIG RLC, disable and enable it, or reseat it if necessary.

Symptom	What to do
There is no dial tone when pressing either the host call appearance or local call appearance keys. (continued)	**6** Contact your telecom administrator. There might be problems at the host PBX.
Lamps or indicators are not lit after completion of a Remote Office 9150 unit power cycle.	**1** Check all cable connections to and from the Remote Office 9150 unit and ensure they are all securely connected. **2** Is this a first-time installation? If yes, check the telephone connections. Refer to the Telco 1 and Telco 2 cable pin-out tables in Appendix D, “Connection pin-out tables.” **3** Ensure the ISDN BRI line is working. Ask your service provider to check this. **4** Check the IP network and ensure that ■ it is not down ■ traffic is being routed between the Remote Office 9150 unit and MIG RLC on the host PBX **5** Ping the MIG RLC from the Remote Office 9150 unit to verify IP network connectivity.
Lamps or indicators do not reflect the true status of the telephone.	It is possible that there is a synchronization error between the Remote Office 9150 unit and the host PBX. Contact your telecom network administrator.
The display is blank (that is, the time and date are not displayed).	**1** Take the digital telephone handset off hook and dial the Online SPRE code. The Remote Office 9150 unit attempts to connect to the host PBX. When the connection is established, the time and date appear.

Symptom	What to do
The display is blank (that is, the time and date are not displayed). (continued)	**2** Check the IP network and ensure that ■ it is not down ■ traffic is being routed between the Remote Office 9150 unit and MIG RLC on the host PBX **3** Ping the MIG RLC from the Remote Office 9150 unit to verify IP network connectivity. **4** Ensure the ISDN BRI line is working. Ask your service provider to check this. **5** Restart the MIG RLC, wait one minute, and then restart the Remote Office 9150 unit. **6** Ensure the MIG RLC is enabled in its host PBX slot. In Load 97 on the Meridian 1 PBX, stat the MIG RLC, disable and enable it, or reseat it if necessary. **7** Contact your telecom administrator. There might be problems at the host PBX.
There are noticeable gaps or poor quality when a voice call is active on the IP network.	**1** Check the Quality of Service configuration on the MIG RLC. Adjust the configuration, if required. Lower the QoS threshold so that transition occurs earlier. **2** Conduct a traffic study on your voice and IP network traffic patterns as described in Appendix A, “Network engineering guidelines.” It is possible that your IP network capacity cannot accommodate the additional voice data, especially during High Day Busy Hour (HDBH) periods. Make adjustments to your network as required.

Symptom	What to do
Incoming calls are not being received from the host PBX.	**1** Ensure your telephone is not on call forward. **2** Ensure the Remote Office 9150 unit is not in offline mode by entering the Online SPRE code at a digital telephone. **3** Ensure the Remote Office 9150 unit is powered up. It cannot receive calls from the host PBX if it is not powered up. **4** Ensure the MIG RLC is correctly configured with your Remote Office 9150 unit's IP address, telephone number, and security ID (if they are used). **5** Ensure the ISDN BRI line is working, if it is being used to route host-controlled calls. Ask your service provider to check this. **6** Check the IP network (if it is being used) and ensure that ■ it is not down ■ traffic is being routed between the Remote Office 9150 unit and MIG RLC on the host PBX **7** Ping the MIG RLC from the Remote Office 9150 unit to verify IP network connectivity. **8** If the problem persists, contact your telecom administrator or Nortel Networks distributor.
Incoming calls are not being received from the PSTN.	**1** Ensure your telephone is not on call forward. **2** Ensure the calling party has your office's correct telephone number. **3** Ensure the Remote Office 9150 unit is powered up. It cannot receive calls from the host PBX or the PSTN if it is not powered up.

Symptom	What to do
Incoming calls are not being received from the PSTN. (continued)	**4** Ensure the ISDN BRI line is working. Ask your service provider to check this. **5** If the problem persists, contact your telecom administrator or Nortel Networks distributor.
A call in progress was suddenly disconnected.	**1** Does your telephone display “Offline Mode?” If so, enter the Online SPRE code to go back online. **2** Contact your telecom and data network administrators. Perhaps network problems caused the call to drop.

Device connectivity

Introduction

This section identifies some problems that can occur on the data network, and describes what to do to resolve them.

Symptom descriptions

If you are not able to establish or maintain data network connectivity, perform troubleshooting as described in the following table.

Note: To enable valid loopback testing of serial ports and cables, Nortel Networks recommends that you use a breakout box.

Symptom	What to do
`SERIAL CONNECTION FAILED` appears when attempting to connect to the Remote Office 9150 unit.	**1** Ensure that you entered the logon ID and password correctly when trying to establish the connection. **2** Ensure that someone else is not already logged on to the Remote Office 9150 unit. **3** Ensure that you selected the correct COM port when trying to establish the connection. **4** Verify that no other applications on the administration PC are using the COM port. **5** Verify that the serial connection is good. **6** Using a breakout box, verify that the COM port is active. **7** Ensure the Remote Office 9150 unit is powered up. **8** Power the Remote Office 9150 unit off, and then back on. **9** Contact your Nortel Networks distributor. There might be a hardware problem.

Symptom	What to do
`10060 TELNET CONNECTION FAILED` appears when attempting to connect to the Remote Office 9150 unit.	**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 that someone else is not already logged on to the Remote Office 9150 unit. **4** Verify that the Ethernet cable is connected at both ends (the Remote Office 9150 unit and the network hub). **5** Check the Ethernet cable and ensure it is good. **6** Ensure the Remote Office 9150 unit is powered up. **7** Power the Remote Office 9150 unit off, and then back on. **8** Ensure the Remote Office 9150 unit's IP address, network mask, and default gateway are correctly configured in the Remote Office 9150 unit. **9** Ping the Remote Office 9150 unit to see if it responds. **10** If the Remote Office 9150 unit does not respond, ping the Remote Office 9150 unit's gateway to see if it responds. **11** If the gateway does not respond, ping a known good device on the Remote Office 9150 unit's network. **12** If steps 10 and 11 work, but step 9 did not, there might be a gateway configuration error. Contact your data network administrator. **13** Contact your Nortel Networks distributor. There might be a hardware problem.

Symptom	What to do
There are many collisions on the Ethernet network, as indicated by a 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 Remote Office 9150 unit 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 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 Remote Office 9150 unit will not send or receive Ethernet traffic.	**1** Ensure that the Remote Office 9150 unit is powered up. The Remote Office 9150 unit cannot send or receive traffic if it is not powered up. **2** Check the Ethernet cable between the Remote Office 9150 unit and the network, and ensure that it is good. **3** Ensure the Ethernet cable is connected. **4** If the Remote Office 9150 unit still will not send or receive traffic, contact your data network administrator. **5** Data network administrator: Ensure that other network devices are configured to allow traffic to and from the Remote Office 9150 unit.
An attempt to log off from the Remote Office 9150 unit does not work.	It is possible that communication has been lost between the administration PC and the Remote Office 9150 unit. Close Configuration Manager, and then restart it.

Symptom	What to do
The Remote Office 9150 unit cannot establish a connection with the MIG RLC.	**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 (as appropriate). **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 MIG RLC. For instructions, see "Using Configuration Manager's Ping" on page 366. **7** If the MIG RLC 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, then 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 ■ 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 Remote Office 9150 unit 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 Remote Office 9150 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 firmware. Perform the configuration upload using a previous configuration file, if necessary. **Note:** Each time you perform a firmware upgrade, you should also create a backup of the configuration. The configuration database format in the Remote Office 9150 unit is dependent on the version of firmware installed. If you recently downgraded to a previous version of 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 Remote Office 9150 unit. Close Configuration Manager, and then restart it.
Nothing happens when attempting to log off from the Remote Office 9150 unit.	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

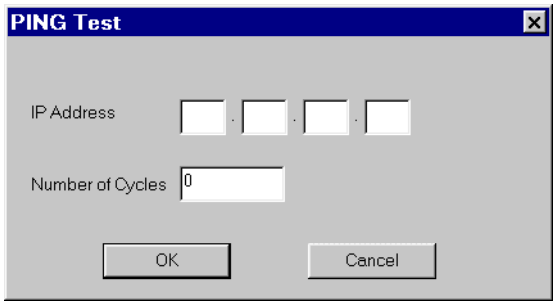
This section explains how to use the Ping option provided in Configuration Manager to verify network connectivity. Use this test as a troubleshooting tool to determine if you can reach the MIG RLC, another remote unit, or any other device on the network.

Getting there 9150 → Configuration Manager

To perform a Configuration Manager ping

1 From the menu, choose Tests → Ping.

Result: The PING Test dialog box appears.



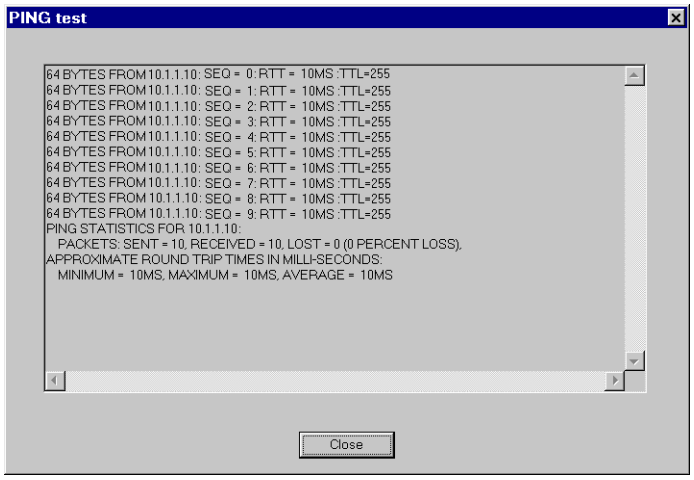
2 Enter the IP Address of the unit you want to ping.

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

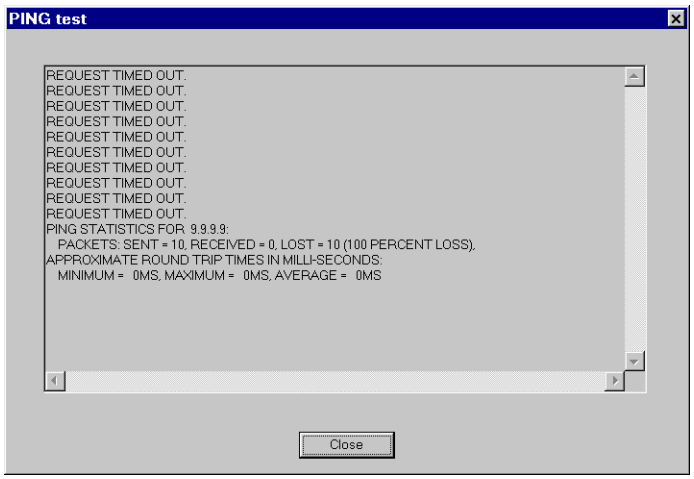
The number must be in the range of 1–100.

4 Click OK.

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



The following is an example of an unsuccessful ping:



5 Click Close.

Result: The Ping test screen closes.

What to do if the ping did not work

1. Ensure that you entered the IP address correctly.
2. Ensure that the subnet mask and default gateway are properly configured on the device you are pinging.

   Confirm this by viewing the IP Configuration property sheet for the device.
3. Ping the device's gateway.
4. If the gateway does not respond, ping a known good device on the device's network.
5. Contact your data network administrator. There may be a configuration error elsewhere on the network.

Recovering from 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

If your Remote Office 9150 unit fails to operate, consult with 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 375

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 386 outlines how you can make this check.

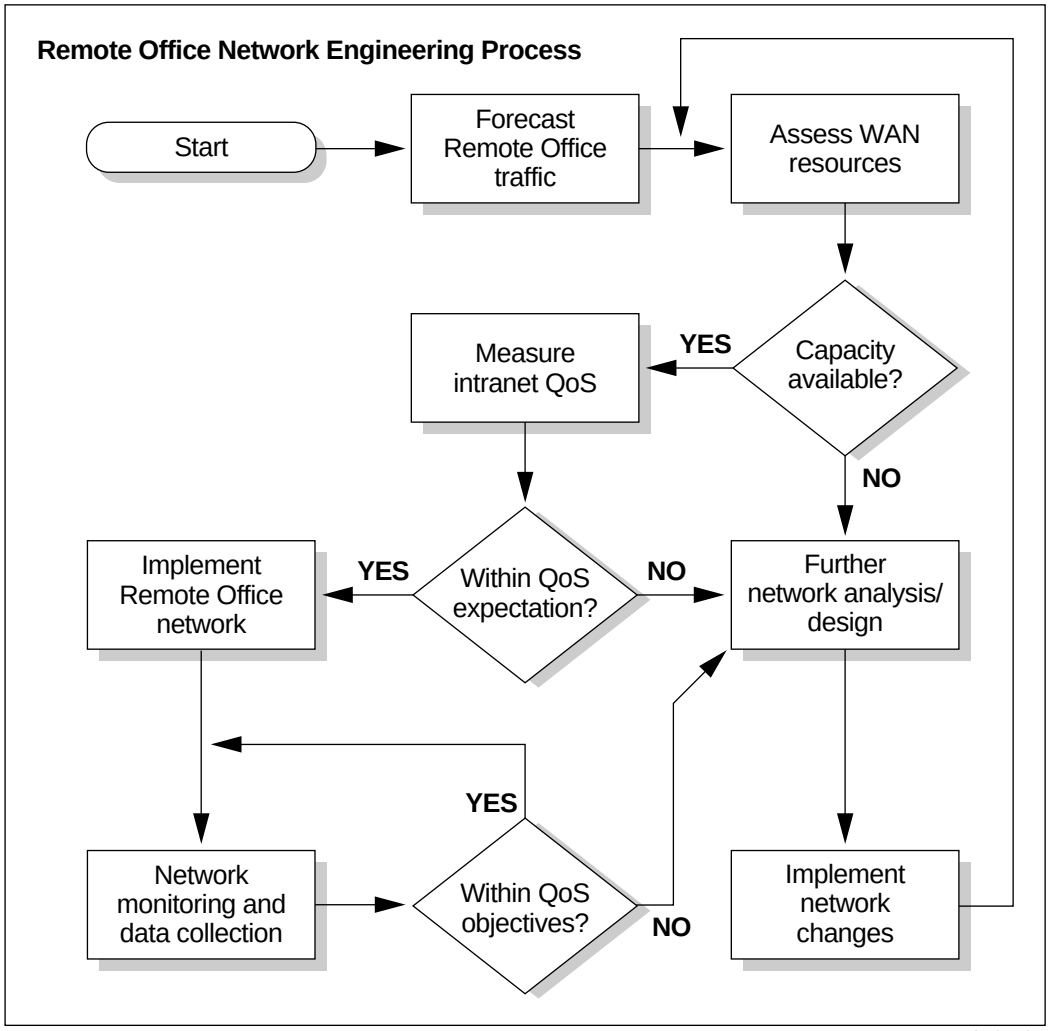
3. Measure the existing intranet’s Quality of Service (QoS).

   You must estimate the quality of voice service the corporate intranet can deliver. “Measuring the intranet Quality of Service” on page 403 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 408 and “Implementing Quality of Service in IP networks” on page 416 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 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 376 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 (telephone sets) 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 376. 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 376, 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 398.

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 376.)
- 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.

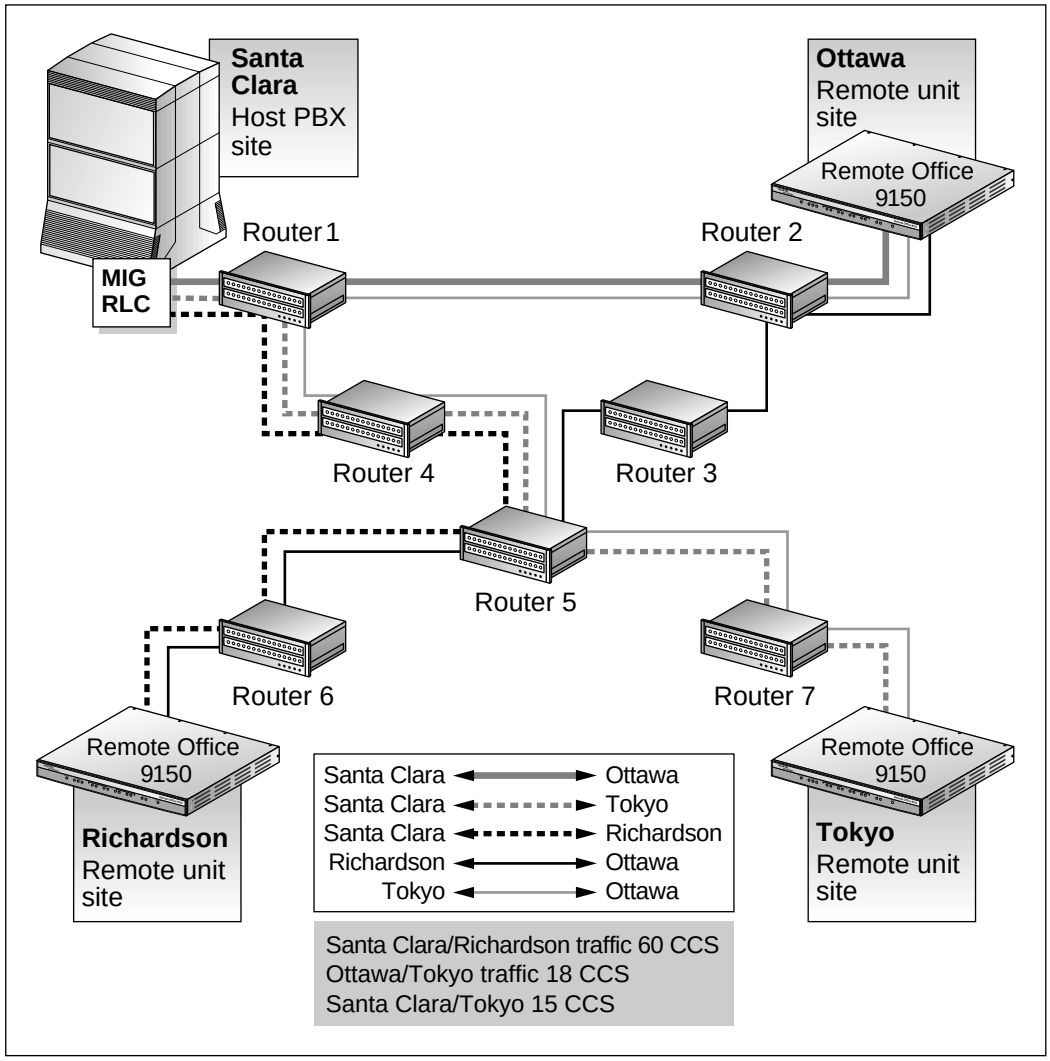
Determining the state of WAN links

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 387. Alternatively, use the traceroute tool. See “Measuring the intranet Quality of Service” on page 403.

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 375), 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 387 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 working 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 394 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

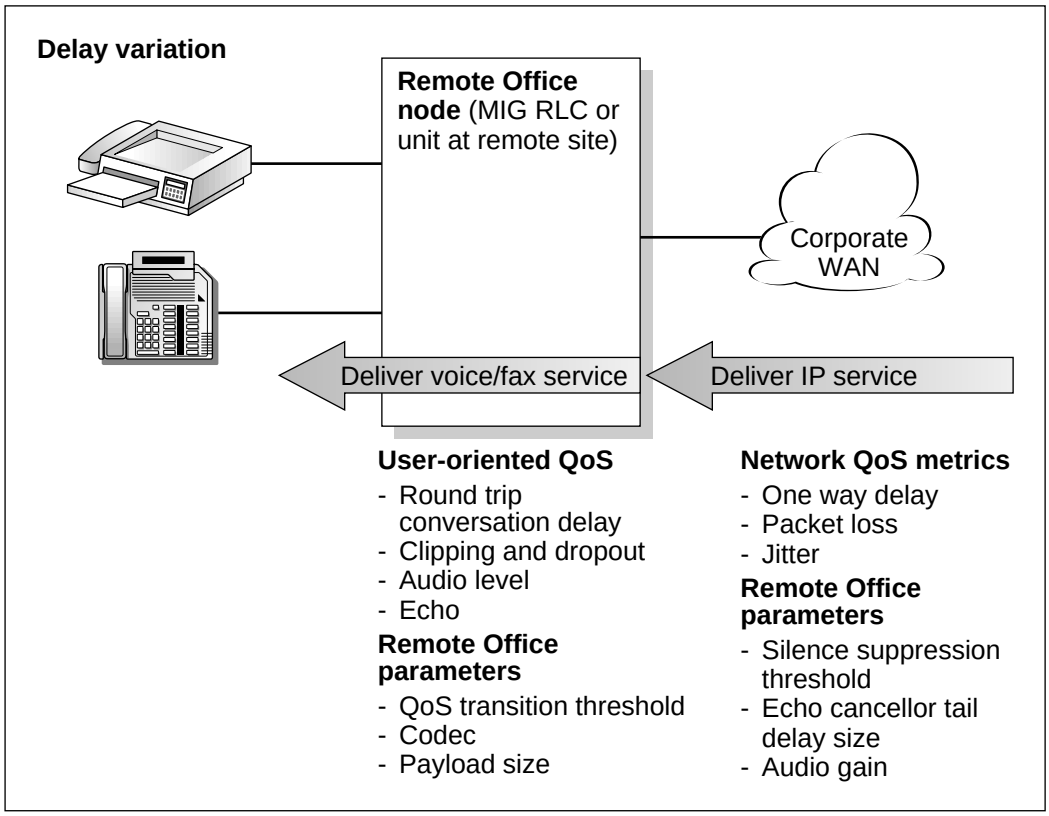
The users of corporate voice and data services expect these services to meet some perceived QoS, which, in turn, influences network design. The goal is to design and allocate enough resources in the network to meet the users' needs. QoS metrics or parameters are what quantify the needs of the service user.

Relationship between users and services

In the context of a Meridian 1 and Remote Office system, the diagram on page 399 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*.



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

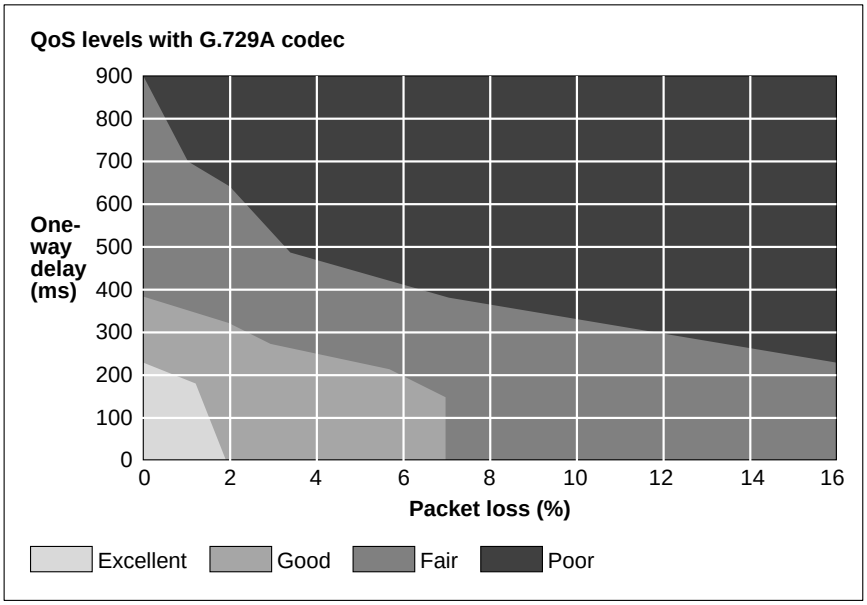
When the QoS level is below the transition threshold, calls to that destination are rerouted over circuit-switched voice facilities. When QoS returns to a point above the set threshold, calls are restored to the IP network.

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.

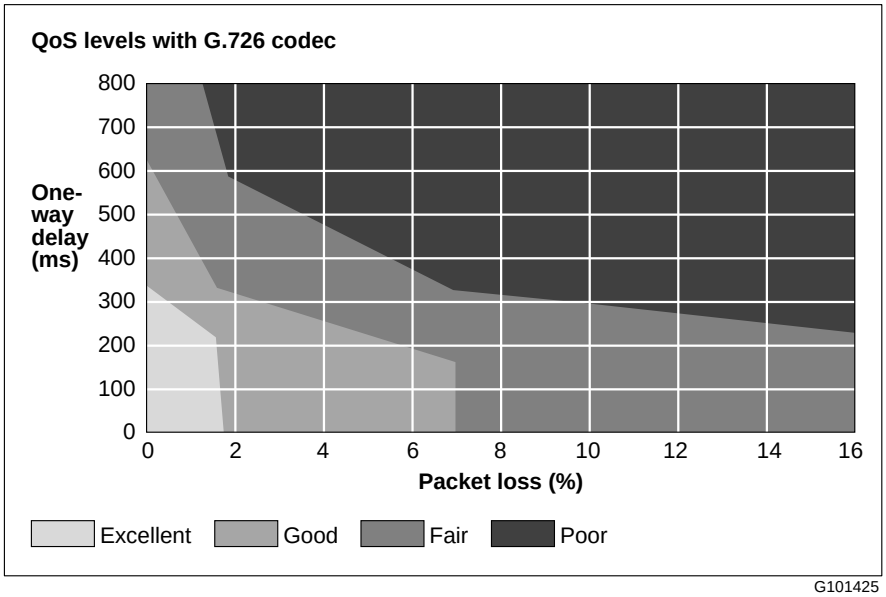
Quality of Service levels by codec

The QoS level graphs on pages 401 and 402 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.

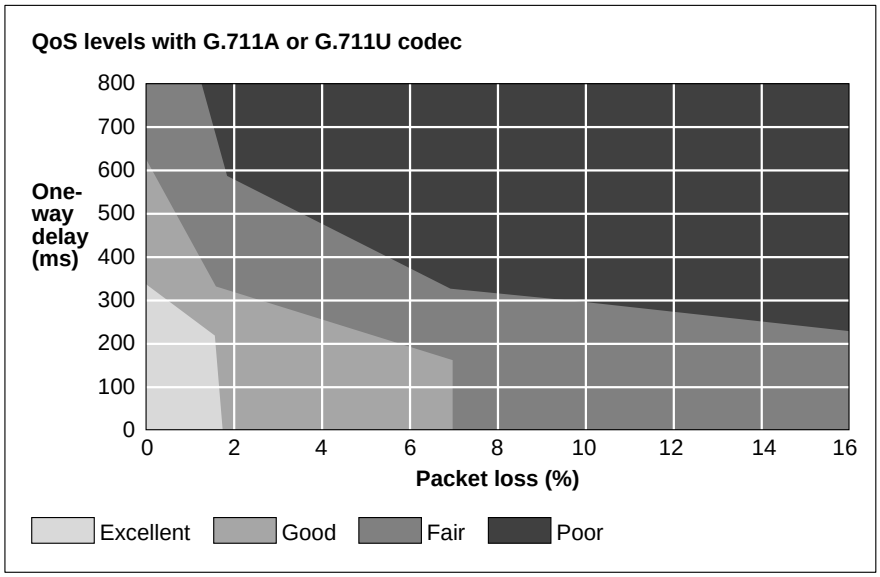
Fax is more susceptible to packet loss than the human ear. Quality starts to degrade when packet loss exceeds 10%. Nortel Networks recommends that fax services be supported with the Remote Office operating in either the Excellent or Good QoS level. Avoid offering fax services between site pairs that can guarantee no better than a Fair or Poor QoS level.



G101424



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 program 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 command 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 the 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 375.

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 406.

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 needs to be reduced to raise the QoS level. “Fine-tuning the network Quality of Service” on page 408 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

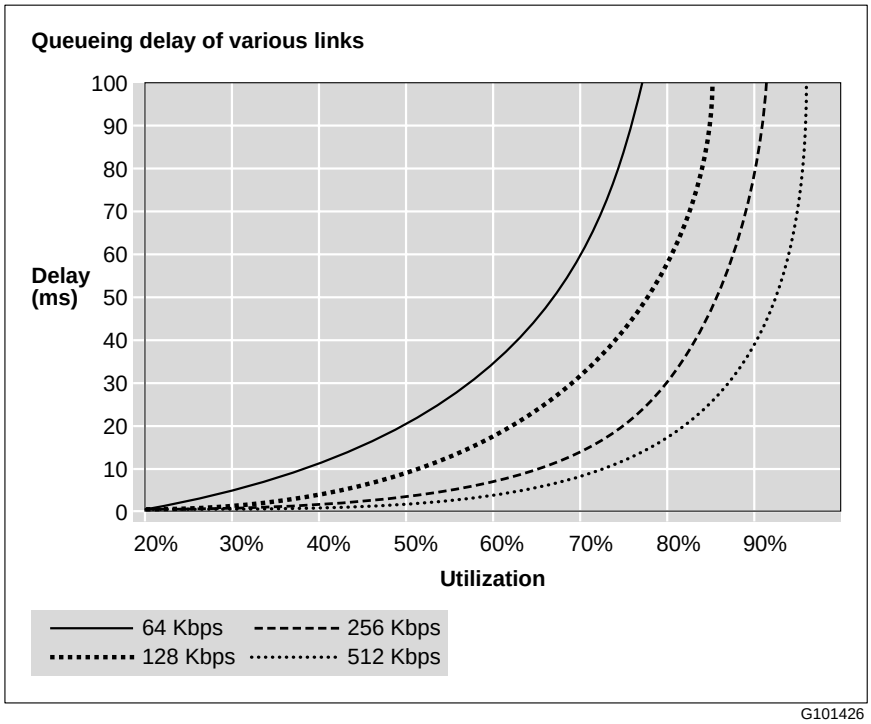
p*p*(average intranet packet in bytes)/(1-p)/(link speed in Kbps),

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 410 displays the average queueing delay of the network based on a 300-byte average packet size.



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 approximately a few milliseconds.

- LAN segment delay

  The transmission and processing delay of packets through a healthy LAN subnet 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 409 and “Queuing delay” on page 410. 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 418.

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 410. 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, improves 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 is 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 410, 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 417 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 recovery transition. 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 a Remote Office 9150 unit at your site. For your reference, forms are also provided for the Meridian Internet Gateway Reach Line Card (MIG RLC).

Network planning

To help you plan your Remote Office network, study the network diagram and sample configurations provided in Appendix C, “Sample configuration files.” The information provided in this appendix demonstrates the relationships between MIG RLC and 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 “Planning the configuration” on page 101.

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 426
- “Completing the MIG RLC forms” on page 442

Section A: 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

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

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

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

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

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

Module 5 (continued)

B-channel 2	DN:		SPID:	
	_____		_____	
	Allocation:		Connection type:	
	❒ Permanent	❒ Demand	❒ Local	❒ Local and Remote
			❒ Remote	
	Trunk group:		Trunk access code:	
	_____		_____	

Module 6

ISDN line type (variant):			Switch type:	
_____			_____	
B-channel 1	DN:		SPID:	
	_____		_____	
	Allocation:		Connection type:	
	❒ Permanent	❒ Demand	❒ Local	❒ Local and Remote
			❒ Remote	
	Trunk group:		Trunk access code:	
	_____		_____	
B-channel 2	DN:		SPID:	
	_____		_____	
	Allocation:		Connection type:	
	❒ Permanent	❒ Demand	❒ Local	❒ Local and Remote
			❒ Remote	
	Trunk group:		Trunk access code:	
	_____		_____	

Remote Office 9150

Configuration Information—ISDN BRI Modules

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

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

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

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

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

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. _____

Section B: 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 426.

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 426.

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 MCAs to transmit data must be assigned to PBX data ports. Users who are 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.

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

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

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

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.

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 464
- data port: on page 466

Sample configuration printouts for the MIG RLC and Remote Office 9150 unit are shown as follows:

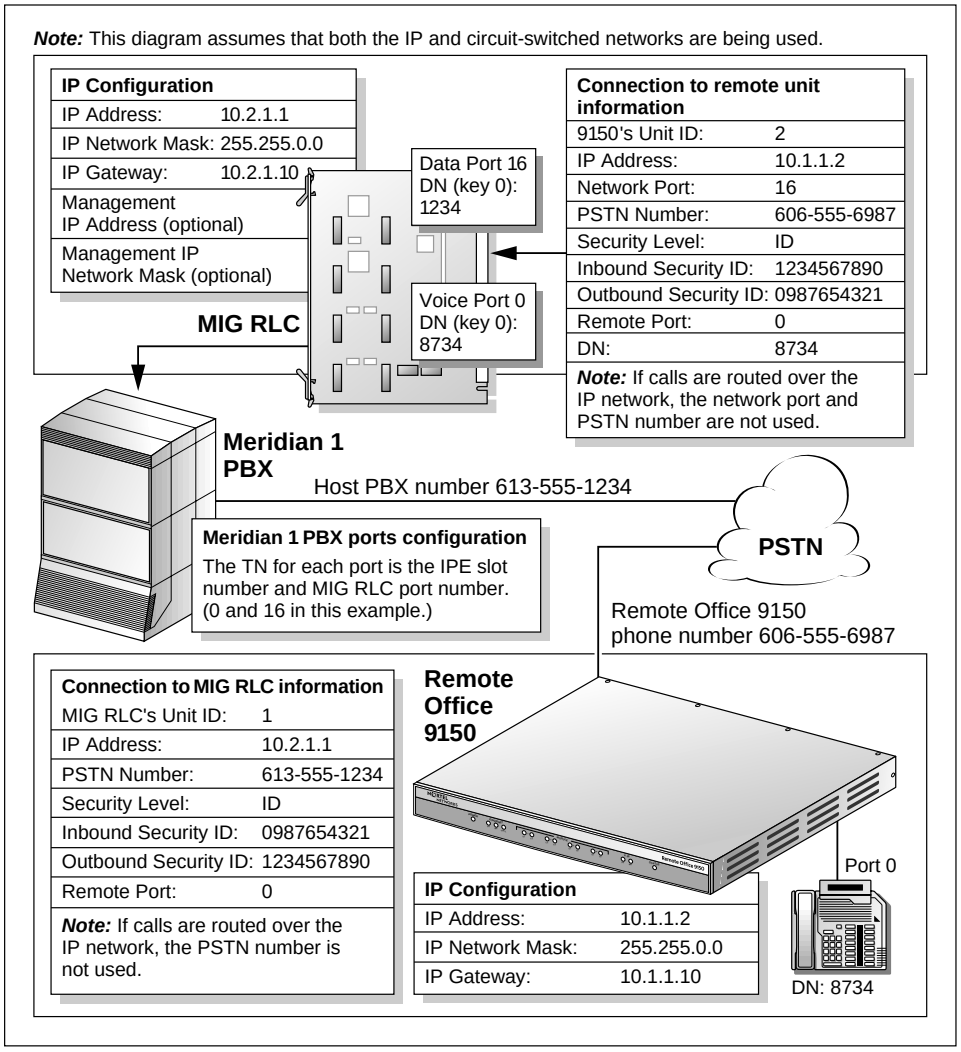
- MIG RLC: on page 468
- Remote Office 9150 unit: on page 472

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 141. 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



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 463.

Note: This configuration example is from a Meridian 1 Option 11.

```
REQ: prt
TYPE: 2616
MARP NOT ACTIVATED

TN   5 0
DATE
PAGE
DES

DES  Bryan Dion
TN   005 0 00 00
TYPE 2616
CDEN 8D
CUST 0
AOM  0
FDN
TGAR 1
LDN  NO
NCOS 0
SGRP 0
RNPG 0
SCI  0
SSU
XLST
```

Telephone type

MIG RLC slot and port numbers

```
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 463.

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

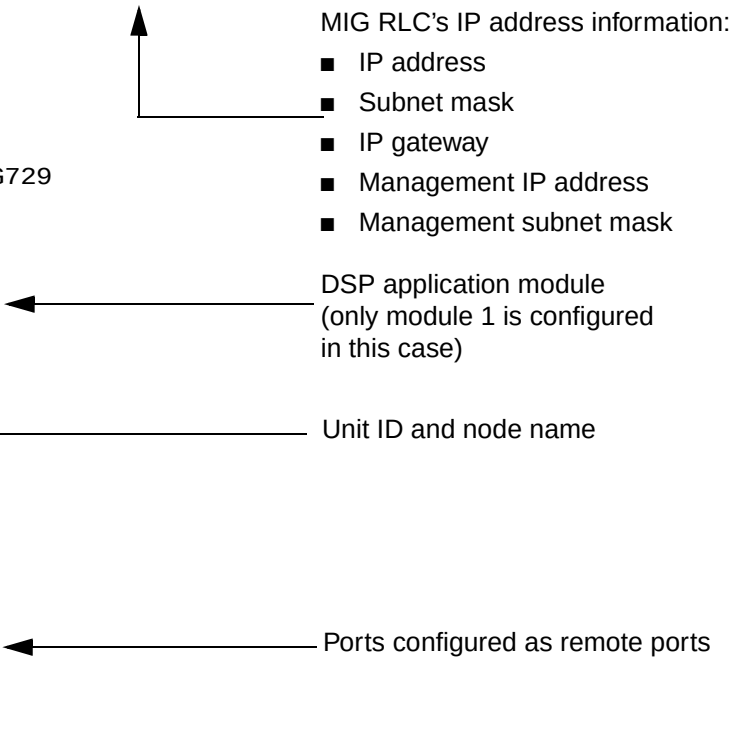
This section shows the configuration settings for the MIG RLC. You can obtain a similar configuration printout by performing a configuration download while connected to the MIG RLC.

Note: Configuration settings are separated by commas (,).

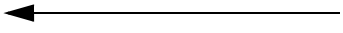
Configuration example

This configuration example uses the settings identified in the network diagram shown on page 463.

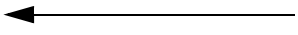
```
IPCFG 10.2.1.1,255.255.0.0,10.2.1.10,10.3.1.2,255.255.0.0

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

SYSCFG 1,HOST1

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
```



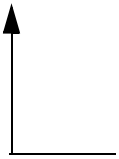
```
PORTCFG 6,0
PORTCFG 7,0
PORTCFG 8,0
PORTCFG 9,0
PORTCFG 10,0
PORTCFG 11,0
PORTCFG 12,0
PORTCFG 13,0
PORTCFG 14,0
PORTCFG 15,0

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

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
```



Ports configured as local ports



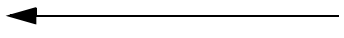
Port configured as network port



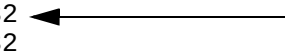
Remote unit connection information (unit 1):

- remote unit number
- 9150's unit ID
- security information (inbound and outbound security IDs)
- remote unit's IP address
- network port
- PSTN number

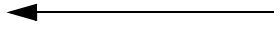
```
ONOFFCFG 1,SUN,0 00:00
ONOFFCFG 1,MON,0 00:00
ONOFFCFG 1,TUE,0 00:00
ONOFFCFG 1,WED,0 00:00
ONOFFCFG 1,THU,0 00:00
ONOFFCFG 1,FRI,0 00:00
ONOFFCFG 1,SAT,0 00:00
ONOFFCFG 2,SUN,0 00:00
ONOFFCFG 2,MON,0 00:00
ONOFFCFG 2,TUE,0 00:00
ONOFFCFG 2,WED,0 00:00
ONOFFCFG 2,THU,0 00:00
ONOFFCFG 2,FRI,0 00:00
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
```



```
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

Item not Configured
```



Quality of Service settings (these are default settings)



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 463.

```
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

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
```

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

Caller ID (not configured)

Appendix D

Connection pin-out tables

In this appendix

TELCO 1 connector pin-out table

Note: The colors shown in this table represent standard telephone cable pin-outs.

Port or module	Pin #	Signal	Color	Pin #	Signal	Color
Digital port 0	1	DP 0 RING	BL-W	26	DP 0 TIP	W-BL
Digital port 1	2	DP 1 RING	OR-W	27	DP 1 TIP	W-OR
Digital port 2	3	DP 2 RING	GR-W	28	DP 2 TIP	W-GR
Digital port 3	4	DP 3 RING	BR-W	29	DP 3 TIP	W-BR
Digital port 4	5	DP 4 RING	SL-W	30	DP 4 TIP	W-SL
Digital port 5	6	DP 5 RING	BL-R	31	DP 5 TIP	R-BL
Digital port 6	7	DP 6 RING	OR-R	32	DP 6 TIP	R-OR
Digital port 7	8	DP 7 RING	GR-R	33	DP 7 TIP	R-GR
Digital port 8	9	DP 8 RING	BR-R	34	DP 8 TIP	R-BR
Digital port 9	10	DP 9 RING	SL-R	35	DP 9 TIP	R-SL
Digital port 10	11	DP 10 RING	BL-B	36	DP 10 TIP	B-BL
Digital port 11	12	DP 11 RING	OR-B	37	DP 11 TIP	B-OR
Digital port 12	13	DP 12 RING	GR-B	38	DP 12 TIP	B-GR
Digital port 13	14	DP 13 RING	BR-B	39	DP 13 TIP	B-BR
Digital port 14	15	DP 14 RING	SL-B	40	DP 14 TIP	B-SL
Digital port 15	16	DP 15 RING	BL-Y	41	DP 15 TIP	Y-BL
Leave open for UL spacing requirements	17	Open	OR-Y	42	Open	Y-OR
Module 4 (ISDN BRI—ST only)	18	MOD 3 Tip 0+	GR-Y	43	Module 3 Tip 0-	Y-GR

Port or module	Pin #	Signal	Color	Pin #	Signal	Color
Module 4 (ISDN BRI—U or ST)	19	MOD 3 Ring 0+	BR-Y	44	Module 3 RING 0-	Y-BR
Module 5 (ISDN BRI—ST only)	20	MOD 4 Tip 0+	SL-Y	45	Module 4 Tip 0-	Y-SL
Module 5 (ISDN BRI—U or ST)	21	MOD 4 Ring 0+	BL-V	46	Module 4 RING 0-	V-BL
Module 5 (for future use)	22	MOD 4 Tip 1+	OR-V	47	Module 4 TIP 1-	V-OR
Module 5 (for future use)	23	MOD 4 Ring 1+	GR-V	48	Module 4 RING 1-	V-GR
Leave open for UL spacing requirements	24	Open	BR-V	49	UK Ring	V-BR
Analog port	25	AP TIP	SL-V	50	AP RING	V-SL

TELCO 2 connector pin-out table

Note: The colors shown in this table represent standard telephone cable pin-outs.

Port or module	Pin #	Signal	Color	Pin #	Signal	Color
Digital port 16	1	DP 16 RING	BL-W	26	DP 16 TIP	W-BL
Digital port 17	2	DP 17 RING	OR-W	27	DP 17 TIP	W-OR
Digital port 18	3	DP 18 RING	GR-W	28	DP 18 TIP	W-GR
Digital port 19	4	DP 19 RING	BR-W	29	DP 19 TIP	W-BR
Digital port 20	5	DP 20 RING	SL-W	30	DP 20 TIP	W-SL
Digital port 21	6	DP 21 RING	BL-R	31	DP 21 TIP	R-BL
Digital port 22	7	DP 22 RING	OR-R	32	DP 22 TIP	R-OR
Digital port 23	8	DP 23 RING	GR-R	33	DP 23 TIP	R-GR
Digital port 24	9	DP 24 RING	BR-R	34	DP 24 TIP	R-BR
Digital port 25	10	DP 25 RING	SL-R	35	DP 25 TIP	R-SL
Digital port 26	11	DP 26 RING	BL-B	36	DP 26 TIP	B-BL
Digital port 27	12	DP 27 RING	OR-B	37	DP 27 TIP	B-OR
Digital port 28	13	DP 28 RING	GR-B	38	DP 28 TIP	B-GR
Digital port 29	14	DP 29 RING	BR-B	39	DP 29 TIP	B-BR
Digital port 30	15	DP 30 RING	SL-B	40	DP 30 TIP	B-SL
Digital port 31	16	DP 31 RING	BL-Y	41	DP 31 TIP	Y-BL
Leave open for UL spacing requirements	17	Open	OR-Y	42	Open	Y-OR
Module 6 (ISDN BRI—ST only)	18	MOD 5 Tip 0+	GR-Y	43	Module 5 Tip 0-	Y-GR

Port or module	Pin #	Signal	Color	Pin #	Signal	Color
Module 6 (ISDN BRI—U or ST)	19	MOD 5 Ring 0+	BR-Y	44	Module 5 Ring 0-	Y-BR
Module 7 (ISDN BRI—ST only)	20	MOD 6 Tip 0+	SL-Y	45	Module 6 Tip 0-	Y-SL
Module 7 (ISDN BRI—U or ST)	21	MOD 6 Ring 0+	BL-V	46	Module 6 Ring 0-	V-BL
Module 7 (for future use)	22	MOD 6 Tip 1+	OR-V	47	Module 6 Tip 1-	V-OR
Module 7 (for future use)	23	MOD 6 Ring 1+	GR-V	48	Module 6 Ring 1-	V-GR
Leave open for UL spacing requirements	24	Open	BR-V	49	Open	V-BR
Fault Relay Contact 1	25	FLT RLY 1	SL-V	50	FLT RLY 2	V-SL

Ethernet connector pin-out table

Pin number	Signal name	I/O	Description
1	TX+	O	Transmit Clock +
2	TXC	I	Transmit Clock Common (Ground)
3	TX-	O	Transmit Clock -
4	Chassis Ground	I	Shield
5	Chassis Ground	I	Shield
6	RXC	I	Receive Clock Common (Ground)
7	RX+	I	Receive Clock +
8	RX-	I	Receive Clock -

Admin (serial) connector pin-out table

Pin number	Signal name	I/O	Description
1			
2	MMI-RXD	I	MMI RS-232C Receive Data
3	MMI-TXD	O	MMI RS-232C Transmit Data
4			
5	Ground	I	Logic Ground
6			
7			
8			
9			

Power connector pin-out table

Pin number	Signal name	I/O	Current	Description
1	+5V	I	5.0 A	+5v
2	Ground	I		Logic Ground
3	+24V	I	1.5 A	+24v
4	-12V	I	0.1 A	+24v

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 multi-user 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.

Multi-user 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 multi-user 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 indicates that it has finished sending a message, and how the receiving device indicates 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 multi-user or dynamic port

station

A telephone 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 data networks, a switch is 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 2048 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

A

B

C

D

E

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

NORTEL NETWORKS™

How the world shares ideas.

Reader Response Form

Product release 1.0
Remote Office 9150
Installation and Administration Guide
555-8421-215

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

Reader Response Form

Remote Office 9150
Installation and Administration Guide

Toronto Information Products
Nortel Networks
522 University Avenue, 14th Floor
Toronto, Ontario, Canada
M5G 1W7

Product release:	1.0
Publication number:	555-8421-215
Document release:	Standard 1.0
Date:	March 2000

Printed in the United States of America

NORTEL NETWORKS™

How the world shares ideas.