NTDR82AC 555-8421-210

Reach Line Card

Installation and Administration Guide

Product release 1.5 Standard 3.0 July 2004

NORTEL NETWORKS

Reach Line Card

Installation and Administration Guide

Product release:	1.5
Publication number:	555-8421-210
Document release:	Standard 3.0
Date:	July 2004

Publication history

July 2004	This is the Standard 3.0 issue of the *Reach Line Card Installation and Administration Guide* for Remote Office product release 1.5.
October 2001	This is the Standard 2.1 issue of the Reach Line Card Installation and Administration Guide. This issue adds support for Remote Office 911x series units and Meridian Digital Telephone IP Adapter (internal and external).
September 2001	This is the Standard 2.0 issue of the Reach Line Card Installation and Administration Guide. This issue adds support for Remote Office 911x series units and Meridian Digital Telephone IP Adapter (internal and external).
March 2000	This is the Standard 1.0 issue of the *Reach Line Card Installation and Administration Guide.*

Contents

Preface

About this document

In this preface

About this guide

The *Reach Line Card Installation and Administration Guide* (NTP 555-8421-210) is for telecom and data network managers and administrators who plan, install, and manage corporate telecommunications and data networks. This guide contains the following information:

- a detailed description of the Reach Line Card (RLC)
- procedures necessary to properly install, configure, and manage the RLC in a host PBX
- necessary configuration for the host PBX
- troubleshooting procedures for addressing possible problems

This guide assumes that you are familiar with the following:

- basic telecommunications terminology
- basic networking terminology
- PC terminology and operation (specifically, Windows 95, 98, NT Workstation 4.0, Millennium Edition (ME), 2000 Professional, XP [Professional and Home Edition])
- Nortel Networks PBX terminology, functionality, and administration

How to use this guide

This guide provides step by step procedures for installing, configuring, and managing the RLC as a part of your Nortel Networks remote services network. Review this guide before beginning RLC installation and configuration.

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

Product overview

Nortel Networks is pleased to announce the Reach Line Card (RLC). The *Reach Line Card Installation and Administration Guide* provides information on how to configure and maintain your RLC.

A standard RLC works with multiple remote service options to provide Meridian 1, Communication Server 1000 (CS 1000), or Communication Server 2100 (CS 2100) PBX functionality to telephones at one or more remote sites. These sites can be any distance from the host PBX. The RLC is compatible with Remote Office 911x series and 9150 units, and Meridian Digital Telephone Internal and External IP Adapter units.

Currently, only Meridian 1 and CS 1000 PBXs support Remote Office 911x series and Meridian Digital Telephone IP Adapters. CS 2100 PBXs do not support Remote Office 911x series or Meridian Digital Telephone IP Adapters at Remote Office product release 1.5.

An RLC does not require external components at the host PBX location. Simply install the RLC in place of a standard Nortel Networks Extended Digital Line Card (XDLC) and configure it as if it served locally connected telephones. Channels that you do not need for remote service telephones can connect to local telephones. In this way, all channels of the RLC can provide service to your corporate telecommunications network.

To identify and locate documentation for the other elements of your Meridian network, refer to “Related information products” on page xxiv.

Skills you need

Knowledge of, or experience with, the following PC concepts as appropriate to your network is helpful when administering the RLC:

- Microsoft Windows
- software installation
- network configuration

Nortel Networks product knowledge

Knowledge of, or experience with, the following Nortel Networks products and concepts:

- basic administration of a Meridian 1, CS 1000, or CS 2100 PBX (telephone set and XDLC configuration)
- characteristics and principles of XDLC operation
- PBX data calls

Telecommunications knowledge

Knowledge of, or experience with, the following aspects of telecommunications:

- digital telephone set configuration
- ISDN PRI configuration
- trunk configuration
- PBX configuration
- PBX maintenance (SDI operation)
- knowledge of RS-232 signaling

Data networking knowledge

Knowledge of, or experience with, the following aspects of data networking:

- data link (Layer 2 of the OSI model)
  - — IP protocol
  - — routing
- network (Layer 3 of the OSI model)
  - — addressing
  - — traffic analysis and provisioning
  - — configuration
- Voice over IP concepts

Conventions used in this guide

This section describes the symbols and text conventions used in this guide.

Precautionary messages

Note: A "Note" describes the secondary results of procedures or commands, or special conditions that require you to 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.

Instructions for selecting menu options

To simplify the instructions for selecting menu options, this guide abbreviates the selection path. For example, if you must choose Telnet from the Logon Unit menu, under the Connect menu, this guide uses the following style:

From the menu, choose Connect → Logon Unit → Telnet.

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 if you are:

- performing an online configuration (connected to a node by serial port or Telnet)
- performing an offline configuration (not connected to a node)

Example

Getting there RLC → Configuration Manager → IP Configuration

The long instruction for this example is as follows:

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 125.
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 126.

2 In the left pane, click on the plus sign **(+)** beside Configuration Manager to expand the node list.

3 Click on **IP Configuration**.

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

PBX terminology

Throughout this guide, the term "host PBX" refers to any of the following Nortel Networks PBX platforms:

- Meridian 1 PBX
- CS 1000
- CS 2100

Related information products

This section lists sources for additional information related to the RLC. You can order printed documentation and the CD-ROM from your Nortel Networks distributor.

You can also download the documentation in Portable Document Format (PDF) from the Nortel Networks website. To locate these documents, click on the **Technical Documentation** link at the following website:

www.nortelnetworks.com

Note: The information available on the website may supersede the information provided on the CD-ROM.

For further details, refer to *Remote Office and RLC Release Notes* (NTP 555-8421-102).

Printed documents

The following documents provide additional information on the RLC and other elements of a Remote Office system:

Remote Office Network Engineering Guidelines (NTP 555-8421-103)

The *Engineering Guidelines,* written for the installer/administrator, describe how a Remote Office system integrates with existing telecommunications and data networks. This document helps you to ensure that your networks are prepared for Remote Office.

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

The *Release Notes,* written for the installer/administrator, describe the features and known problems for the different elements of a Remote Office system. This document contains information pertaining to the Reach Line Card (RLC), the Remote Office 9150 unit, Remote Office 911x series units, and Meridian Digital Telephone IP Adapter units.

Remote Office 9150 Installation and Administration Guide (NTP 555-8421-215)

The *Remote Office 9150 Installation and Administration Guide*, written for the installer/administrator, describes how to install, configure, and manage the Remote Office 9150 unit.

Remote Office 911x Series Installation and Administration Guide (NTP 555-8421-220)

The *Remote Office 911x Series Installation and Administration Guide,* written for the installer/administrator, describes how to install, configure, and manage Remote Office 911x series units.

Meridian Digital Telephone IP Adapter Installation and Administration Guide (NTP 555-8421-211)

The *Meridian Digital Telephone IP Adapter Installation and Administration Guide,* written for the installer/administrator, describes how to install, configure, and manage Meridian Digital Telephone IP Adapter units.

CD-ROM

A Remote Office Product CD-ROM is available containing the documentation in Portable Document Format (PDF), firmware, and Remote Office Configuration Manager software.

Chapter 1

RLC description

In this chapter

Product introduction

The Reach Line Card (RLC) emulates a standard Extended Digital Line Card (XDLC) and provides Private Branch Exchange (PBX) functionality for telephones at remote locations. The RLC supports up to 20 remote devices (with a limit of eight Remote Office 9150 units for a single RLC). The total number of simultaneous telephone calls cannot exceed the total number of RLC ports in the host PBX. The RLC supports the following devices:

- Remote Office 9110
- Remote Office 9115
- Remote Office 9150
- Meridian Digital Telephone Internal IP Adapter
- Meridian Digital Telephone External IP Adapter

You can configure each port on the RLC as if telephones were locally connected to a standard XDLC. Existing digital trunks (PRI) or an integrated 10BaseT Ethernet interface (Voice over IP) carry voice and signaling traffic as packets.

Note: The RLC defaults to a half-duplex 10BaseT Ethernet connection. You can configure a full-duplex 10BaseT Ethernet connection through Configuration Manager. When you configure a full-duplex 10BaseT Ethernet connection, the RLC's Ethernet collision LED remains on solid (constantly lit). This does not indicate collisions on the segment, but that Full duplex is enabled. In addition, when you enable full-duplex Ethernet, you must also set the corresponding port on the connected switch to 10 FULL Duplex. Remote Office products do not support Auto negotiation of the Ethernet interface.

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

Physical features

The 16-port version of the RLC (NTDR68xx) provides service for up to 16 telephones. At the host location, install a 16-port RLC in an IPE shelf of the host PBX, or the Meridian 1 PBX 11C – Cabinet of a Meridian 1 PBX.

The 32-port version of the RLC (NTDR70xx or NTDR71xx) provides service for up to 32 telephones. At the host location, install a 32-port RLC in an IPE shelf of the host PBX, or the Meridian 1 PBX 11C – Cabinet of a Meridian 1 PBX.

PBX hardware compatibility

The following sections list the RLC's PBX requirements.

Meridian 1 PBX

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

- Meridian 1 PBX 11, 11C – Cabinet, 11C – Chassis, 11E, 51C, 61C, 71C, and 81C

  The RLC is compatible with the Meridian 1 PBX 11C – Chassis with the following limitations:

  — The 16-port RLC is supported in slots 1—3 in the main chassis.

  — The 16-port RLC is supported in slots 7—10 in the expander chassis.

  — The 32-port RLC is supported in slots 1 or 2 in the main chassis, with a maximum of one RLC.

  — The 32-port RLC is supported in slots 7, 8, or 9 in the expander chassis, with a maximum of two RLCs.

  Note: Since the 32-port RLC requires two backplane connections, it cannot be assigned to slot 10, because this slot provides only one backplane connection.

- Older Meridian 1 PBX systems that are upgraded with IPE modules

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

CS 1000

To obtain the RLC requirements for CS 1000 PBXs, contact your Nortel Networks distributor.

CS 2100

The RLC's required packages for CS 2100 PBXs are as follows:

- X11 packages 0 and 121 contain all the four required Classes of Service.
  - — Package Number 0 (Basic Call Processing Package) includes FLXA, VCE, and WTA.
  - — Package Number 121 (Station Camp-on) includes CPTA.
- The following four feature sets of release 25.30 include both packages:
  - — NTSK11CQ: Meridian 1 PBX 11C General Business Feature Set
  - — NTSK11DQ: Meridian 1 PBX 11C Enhanced Business Feature Set
  - — NTSK11EQ: Meridian 1 PBX 11C Enterprise Business Feature Set
  - — NTSK11FQ: Meridian 1 PBX 11C nas/vns Feature Set

IPE vs. Meridian 1 PBX 11

You can purchase 32-port RLCs for both IPE shelves and Meridian 1 PBX 11 cabinets. Because the dimensions of card slots in IPE shelves and Meridian 1 PBX 11 cabinets differ slightly, Nortel Networks offers two varieties of the 32-port RLC. Each variety has its own order code, as outlined in the following table:

Destination	Order code
IPE shelf	NTDR70xx
Meridian 1 PBX 11 cabinet	NTDR71xx

Regardless of order code, the motherboard of the 32-port RLC is the same circuit pack that is used for the 16-port RLC. The illustration on page 6 shows the circuit pack. The RLC motherboard conforms to the Common Features Specification for IPE line cards.

Communications system and software requirements

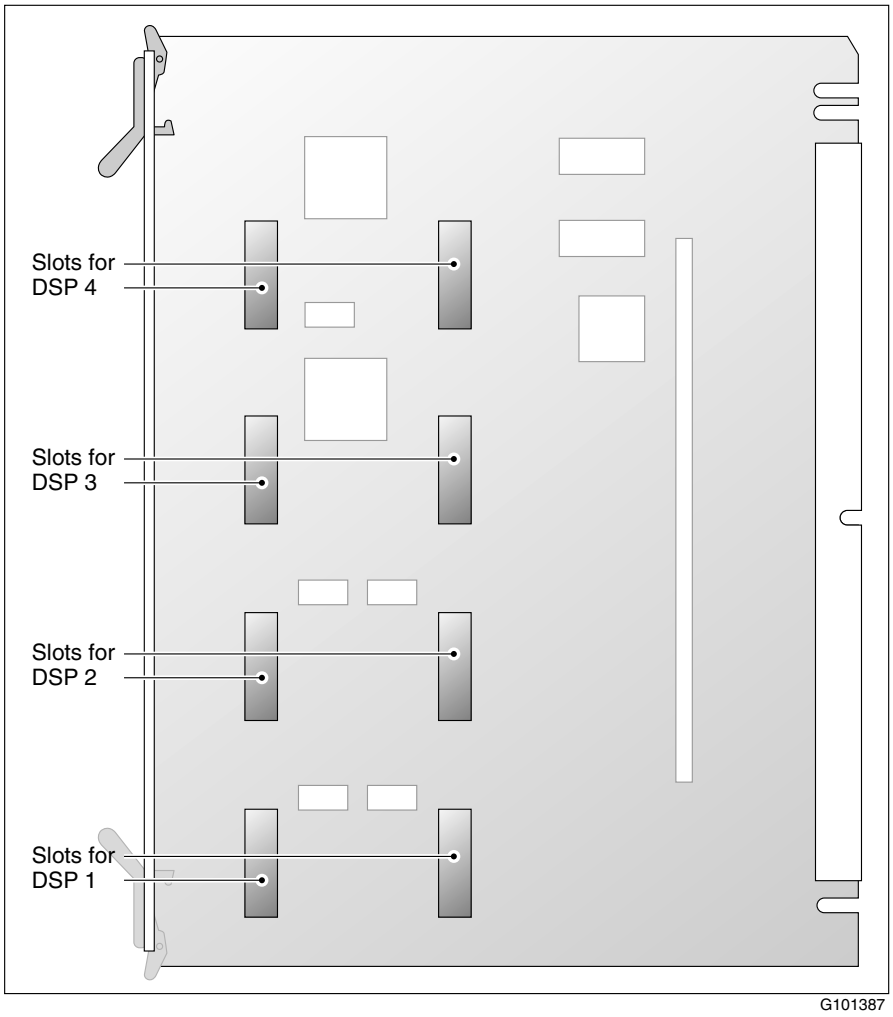
The following table shows the software versions necessary to run RLCs on compatible Nortel Networks' communications systems.

RLCs

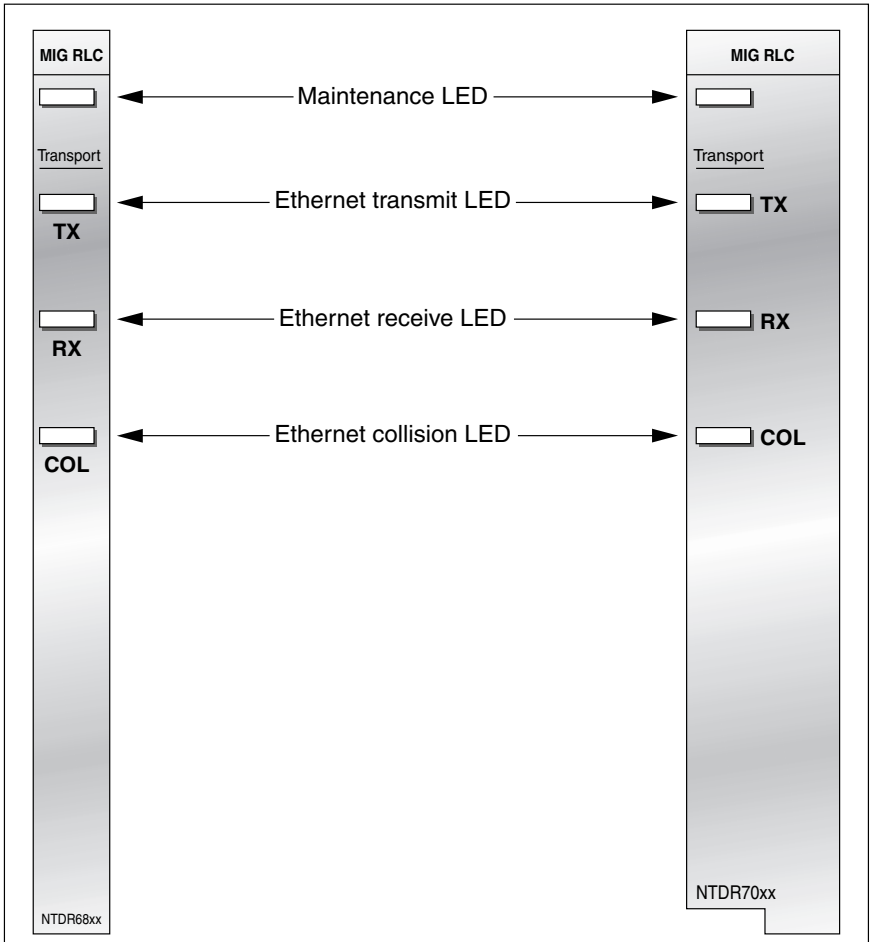
Communications system[i]	System software version
Meridian 1 PBX	X11 release 23 or higher
CS 1000	Release 2 or higher
CS 2100	Release MSL12 or higher

i. Requires Remote Office software version 1.5 or higher.

RLC motherboard



RLC faceplates: 16-port and 32-port



Note: The IPE version of the double-wide faceplate is pictured here. If the RLC is installed in a Meridian 1 PBX 11 cabinet, the order code on the faceplate is NTDR71xx.

G101386

LED indicators

Four faceplate LED indicators monitor the basic health, transmit activity, receive activity, and Ethernet collisions on the RLC. The illustration on page 7 shows the 16- and 32-port RLC faceplates with the function of each LED labeled.

Maintenance

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

Other characteristics of the Maintenance LED include:

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

  After breaking this connection, re-insert the card completely into its slot. If the RLC still does not complete a successful self-test, it must be replaced.

Ethernet Transmit

The green Ethernet Transmit LED indicates the transmission of Ethernet packets by the RLC.

Ethernet Receive

The green Ethernet Receive LED indicates the reception of Ethernet packets by the RLC.

Ethernet Collision

The yellow Ethernet Collision LED indicates a collision on the RLC's Ethernet interface (half-duplex only). Half-duplex Ethernet connections only allow their nodes to either send or receive packets at any given time. Collisions occur when two nodes on a half-duplex Ethernet connection attempt to transmit information simultaneously. Before transmitting, the Network Interface Card (commonly referred to as the NIC card) monitors the line, or listens, for transmissions. A NIC card listens to the line for the amount of time that it takes to transfer a minimum-sized packet the maximum length of the cable. If the NIC card senses no transmission from the destination node, it proceeds with its own transmission.

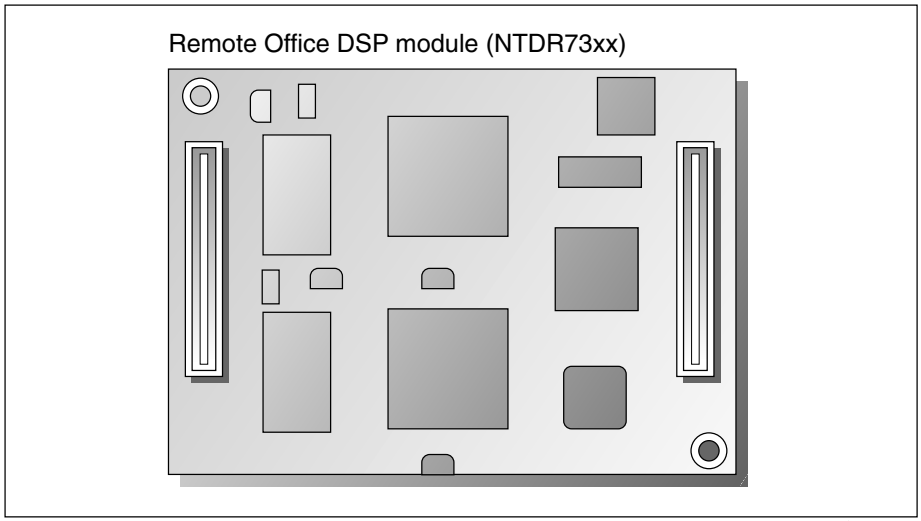
If a NIC card detects a collision, it waits for a period of time determined by the back-off algorithm, then re-transmits the packet. Ethernet nodes keep track of how many times they must re-transmit a packet with a maximum collision re-try counter. In previous versions of Remote Office, the maximum collision re-try counter had a limit of 15. After 16 unsuccessful attempts to transmit a packet (the original attempt plus 15 re-tries) the Remote Office unit dropped the packet. In an effort to decrease delay and improve QoS, the limit of the maximum collision re-try counter is now eight. After nine unsuccessful attempts to transmit a packet (the original attempt plus eight re-tries) the Remote Office unit drops the packet and begins attempting to transmit the next packet.

Note: When you configure the RLC IP interface for full-duplex Ethernet, the Ethernet Collision LED remains on solid (constantly lit). For configuration information, refer to "Full Duplex Ethernet" on page 185.

DSP application modules (NTDR73xx)

The RLC's on-board digital signal processor (DSP) resources provide voice processing for up to eight simultaneous telephone calls. Each DSP application module provides an additional eight channels of packet voice processing. To extend your system's voice processing capacity, you can add up to four DSP application modules. The illustration on page 6 shows the locations of DSP expansion slot pairings on the RLC. For help in determining the number of DSP application modules you need to increase your system's call-processing capabilities to the desired level, refer to "Installing DSP application modules" on page 81, and the RLC "System expansion worksheet" on page 343.

The following illustration shows a DSP application module. One DSP application module holds two DSP devices:



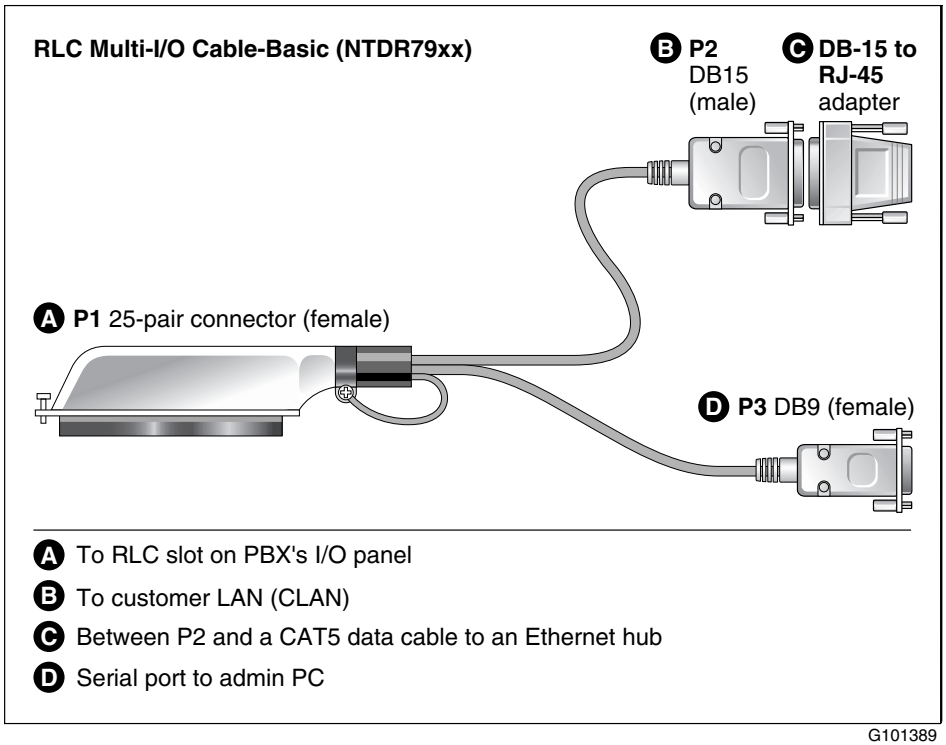
RLC cables

RLC cables connect at the I/O panel of the shelf or cabinet in the host PBX. Nortel Networks offers two cables that enable users to add the RLC to a variety of existing network configurations.

RLC Multi-I/O cable–Basic (NTDR79xx)

The Basic cable provides 10BaseT connectivity to the corporate LAN for Voice over IP (VoIP) and administration access, and RS-232 connection for serial port administration.

Note: The RLC supports only 10BaseT Ethernet speeds.



G101389

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

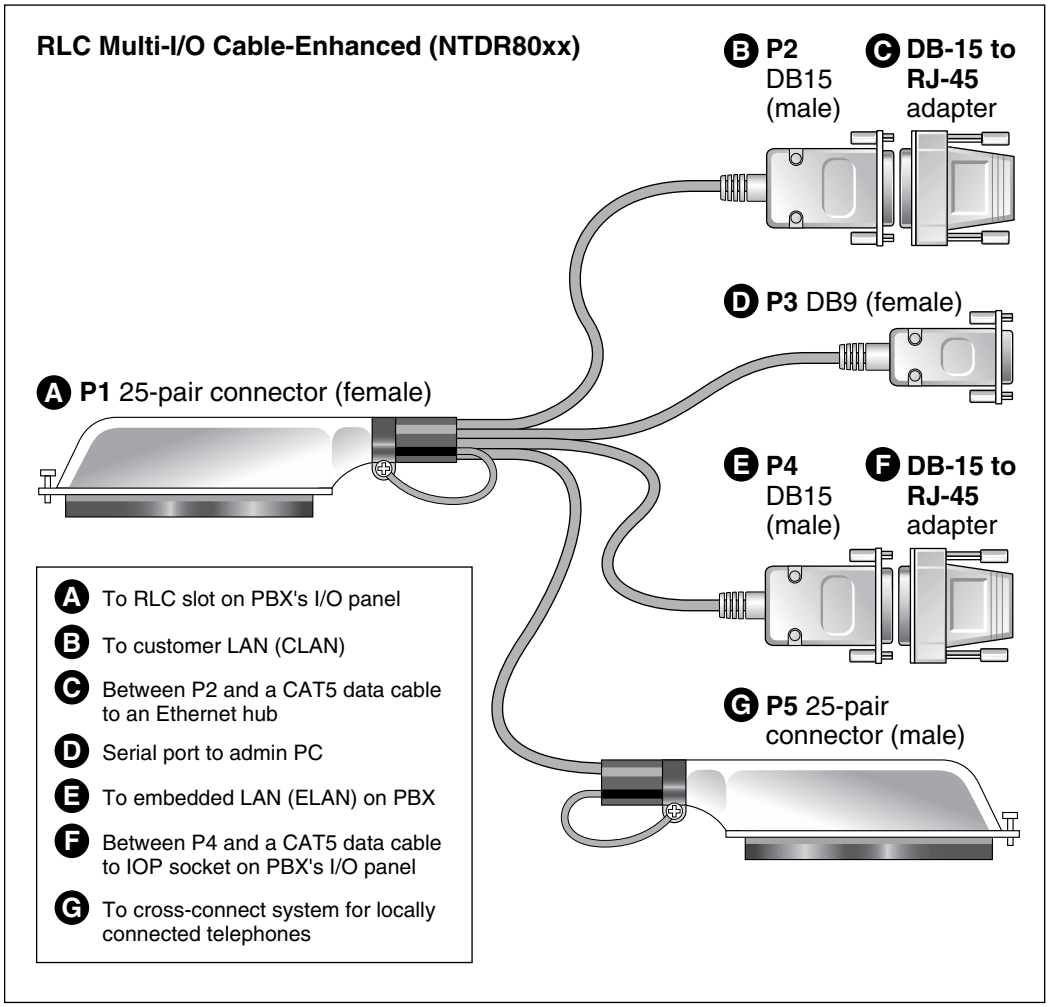
The connector labeled	is a	that transmits	and connects to the
P1	25-pair connector (female)	all signals	I/O panel.
Note: If you are using a 32-port RLC, insert **P1** into the socket for the first of the two card slots occupied by the RLC.			
P2	DB-15 connector (male)	10BaseT signaling	CLAN Ethernet (customer LAN on the network).
Note: P2 requires a DB-15 to RJ-45 converter (part number 301-00001-01, shipped with the cable).			
P3	DB-9 connector (female)	RS-232 signaling	serial port to admin PC for administration and maintenance.

The length of this cable, from the termination end of P1 to the termination end of any other plug, is 0.6 meters (2 feet).

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

The RLC Multi-I/O cable–Enhanced allows you to use the RLC's complete functionality. In addition to the connectivity supplied by the RLC Multi-I/O cable–Basic (refer to page 11), the RLC Multi-I/O cable–Enhanced adds connectivity to the host PBX's internal (or embedded) Ethernet for switch maintenance. With the Enhanced cable you can also service locally connected telephones through RLC ports not used for remote service purposes.

Note: The RLC supports only 10BaseT Ethernet speeds.



G101533

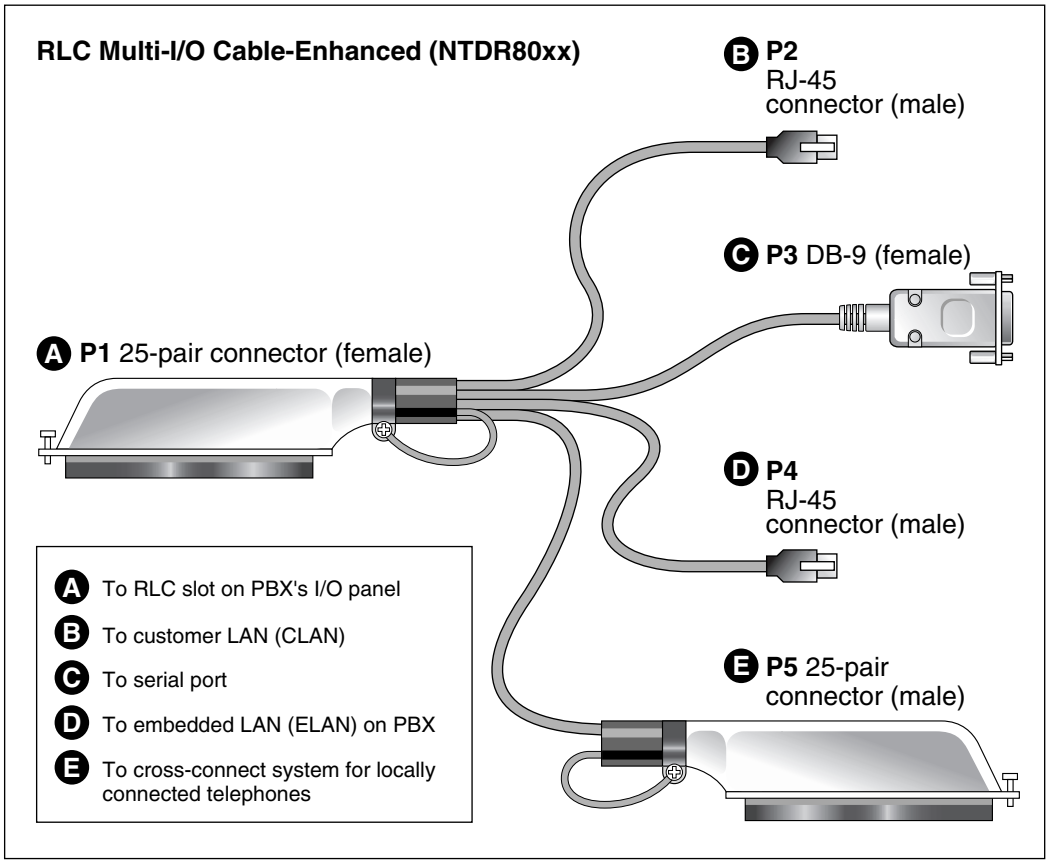
The following table describes the RLC Multi-I/O cable–Enhanced:

The connector labeled	is a	that transmits	and connects to the
P1	female 25-pair connector	all signals	I/O panel.
Note: If you are using a 32-port RLC, insert **P1** into the socket for the first of the two card slots occupied by the RLC.			
P2	male DB-15 connector	10BaseT signaling	CLAN Ethernet (customer LAN on the network).
Note: P2 requires an RJ-45 Male to Female converter (already installed).			
P3	female DB-9 connector	RS-232 signaling	serial port to admin PC for administration and maintenance.
P4	male DB-15 connector	10BaseT signaling	ELAN Ethernet (host PBX's embedded LAN).
Note: P4 requires an RJ-45 Male to Female converter (already installed).			
P5	male 25-pair connector	TCM signaling	cross-connect to local telephones.

The length of this cable, from the termination end of P1 to the termination end of any other plug, is 0.6 meters (2 feet).

Installations outside North America

RLC installations outside North America that use the RLC Multi-I/O cable–Enhanced require the cable shown in the following illustration:



Remote unit capacity on RLCs

One RLC supports a maximum of 20 Remote Office 911x series units or Meridian Digital Telephone Internal or External IP Adapter units.

Note: This scenario requires a 32-port RLC with no other Remote Office units connected to it.

One RLC supports a maximum of eight Remote Office 9150 units when there are no other Remote Office units connected to the RLC.

Note: This scenario requires either a 16- or a 32-port RLC with no other Remote Office units connected to it.

One RLC can also support combinations of Remote Office 9150, Remote Office 911x series, and Meridian Digital Telephone IP Adapter units. The only requirement is that the RLC and Remote Office 9150 unit have enough DSP resources to support the intended call-blocking scenario. For help in determining the number of DSP resources required by your configuration, refer to the "System expansion worksheet" on page 343.

Meridian digital telephone compatibility

The RLC is compatible with the following Meridian digital telephone equipment:

Models		Modules
■ M2006[i]	■ M3310	■ add-on modules[ii]
■ M2008D	■ M3820	■ key-expansion modules
■ M2008HFD	■ M3901[i]	
■ M2216D	■ M3902	
■ M2616D	■ M3903	
■ M2616CT	■ M3904	
■ M3110[i]	■ M3905	

i. Remote Office 911x units and Meridian Digital Telephone IP Adapters do not support M2006, M3110, or M3901 telephones.

ii. Add-on modules include key based add-on modules (KBAs) and display-based add-on modules (DBAs) for M39xx digital telephone sets.

M3901 digital telephone set support

Remote Office allows you to use M3901 digital telephone sets for local (locally controlled) calls or for remote (host-controlled) calls, not both. For local (locally controlled) calls, configure the digital telephone set as an M3901 at both the remote unit and the host PBX. For remote (host-controlled) calls, configure the digital telephone set as an M3901 at the remote unit and as an M3902 at the host PBX.

Footstand

Installation of a Remote Office 9110 unit or a Meridian Digital Telephone Internal IP Adapter unit requires an Analog Terminal Adapter/Meridian Communications Adapter (ATA/MCA) footstand. Meridian Modular Telephones (M2000 series) with a date code of May 6, 1998 or later come equipped with the required footstand. Contact your Nortel Networks distributor to obtain the necessary footstand if your telephone has an earlier date code.

Data channel adapters

The Remote Office 9150 unit supports the following types of data channel adapters:

- Analog Telephone Adapters (ATAs)

  Note: The Remote Office systems using ATAs do not support modems.

- Meridian Communication Adapters (MCAs)

Note: MCAs use the secondary data channel of the TCM telephone interface and require a full 64 Kbps of bandwidth. If you have a 56 Kbps connection, ensure that this connection provides multiple B-channels. Refer to “Understanding port relationships” on page 110 for information about port assignment for data channel adapters.

A 16-port RLC handles up to four data channel adapters. A 32-port RLC handles up to seven data channel adapters.

Note: Remote Office 911x units and Meridian Digital Telephone IP Adapters do not support data channel adapters.

Nortel Networks CTI and ACD applications

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

Classes of service RNGI and RNGB

Remote Office supports classes of service RNGI and RNGB.

- **Class of Service RNGI:** Class of Service RNGI permits digital telephones to ring rather than buzz when they are offhook.
- **Class of Service RNGB:** Class of Service RNGB, like RNGI, applies ringing to digital telephones that are idle but offhook, but unlike RNGI it also applies ringing to digital telephones that are busy and offhook on another line.

Local TCM ports on the RLC support these features. However, digital telephone sets connected to Remote Office units do not support RNGI, RNGB, DRG2, DRG3 or DRG4. Digital telephone sets connected to Remote Office units support DRG1, the default ring.

Note: The RNGI and RNGB features are only available if there are no local calls present on the digital telephone set. If a local call is present on the digital telephone set, the ringer is converted to a beep tone (tone B message).

Operational characteristics

The RLC provides a number of unique features that distinguish it from other remote service products.

These features include:

- adjustable quality of service (QoS) using QoS Transitioning Technology
- port sharing options
- multiple security levels
- packet voice processing
- dial-up trunking
- bandwidth allocation
- Meridian telephone equipment compatibility

Adjustable QoS using QoS Transitioning Technology

Nortel Networks' patented QoS Transitioning Technology monitors the QoS level on the internet protocol (IP) portions of your Remote Office system. This feature detects poor voice QoS when it occurs. The QoS level is a user-oriented metric that takes one of ten settings. Using Configuration Manager, you can select an acceptable transition threshold from among the ten predefined settings to identify the limits of acceptable voice QoS.

Configuring QoS Transitioning Technology to provide satisfactory results requires a detailed understanding of traffic on your IP network. For guidance on evaluating and adjusting your network's QoS, refer to the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103). Refer to page 16 for instructions on obtaining this document.

QoS on shared networks

High volumes of data packets can cause QoS problems for voice traffic on shared networks. Configuring the router to send voice packets ahead of data packets (prioritizing voice packets) can address some QoS concerns. For further details, refer to "Prioritizing voice traffic over shared networks" on page 185.

Port sharing options

The RLC allows you to take maximum advantage of your host PBX's port resources regardless of what time it is or who is working. Dynamic port pooling and multi-user ports allow more than one person or station to use the same port on the host PBX. Dynamic port pooling and multi-user ports allow for more flexible, less restrictive use of the corporate telecommunications network.

Dynamic port pooling

Dynamic port pooling allows multiple users or stations to time-share the same port on the host PBX. No correlation exists between a user or station and the TN or DN on the host PBX when no one is registered.

When users share ports in a dynamic pool register, they receive the next available port in the pool regardless of that port's TN or DN. Users register by entering the Registration SPRE (Special Prefix) code on their telephone keypad. Refer to the Installation and Administration Guide for your specific Remote Office unit for details.

Note: If there are no available ports in the pool when a user tries to register, that user hears a fast busy signal.

When users press the primary DN key on their digital telephone set to place an outgoing call, they receive the DN assigned to them at registration. While registered, users also receive all calls placed to that DN. When users are ready to release their ports on the host PBX, they enter the deregistration SPRE code. This allows registering users to access that port.

Multi-user ports

Like dynamic port pooling, multi-user ports also allow multiple users or stations to time-share ports on the host PBX. With a multi-user port, however, there *is* a specific correlation between the user or physical station and the TN or DN on the host PBX. The host PBX blocks users configured to a multi-user port from accessing that port if another configured user is currently registered to the port. Multi-user ports are available only to users specifically configured to the ports.

While multiple users in a dynamic port pool can be active at the same time, only one user can be active on a multi-user port.

You can configure a multi-user port to allow one user to access the same port from multiple locations. This feature can give one person access the same port from both the corporate office and the home office. Refer to the Installation and Administration Guide for your specific Remote Office unit for details.

Multiple security levels

The RLC allows you to choose from three levels of protection from unauthorized access to your host PBX through the Remote Office system. Select one of the following security levels to regulate usage of corporate telecommunications resources:

- Level 1, no security

  When you set RLC security to security level 1, the RLC allows all calls to route through the host PBX, regardless of source.

  Note: Level 1 is the RLC's default security level.

- Level 2, caller ID security

  When you set RLC security to security level 2, the RLC does the following:

  a. It compares the caller ID of the incoming call against the caller IDs configured for this remote unit.

  b. It denies PBX access to this call if the caller ID does not match any of those in this unit's List of Caller IDs.

  For the required steps to configure security level 2 on your RLC, refer to "Remote connection configuration" on page 197.

  Note: Level 2 security is not applicable when using Remote Office 911x series units with the RLC.

- Level 3, provisioned security

  When security is set to level 3, depending on the unit that initiated the call, the following call verification occurs:

  a. If a remote unit calls the RLC, the RLC compares its Inbound security ID with this remote unit's Outbound security ID. If they match, the RLC accepts the call, otherwise, it rejects the call.

b. If the RLC calls a remote unit, the remote unit compares its Inbound security ID with the RLC's Outbound security ID. If they match, the remote unit accepts the call, otherwise, it rejects the call.

For the steps required to configure security level 3 on your RLC, refer to "Remote connection configuration" on page 197.

Security configuration applies to all ports of a Remote Office unit. That is, all ports on one Remote Office 9150 unit have the protection of the same security level.

Packet voice processing

All connections to the host PBX support the following features:

Voice compression

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

Note: Remote Office 911x units only support G.729A compression in Public Switched Telephone (PSTN) mode. They support G.711 and G.729A in VoIP mode.

Voice jitter attenuation buffer

The RLC's dynamic voice jitter attenuation buffer compensates for the uneven arrival of voice packets at their destinations over a given period of time across data networks. This buffer collects packets that arrive unevenly and relays them evenly.

Packet-loss handling techniques

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

Silence suppression algorithm

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

Echo cancellation

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

Due to the network delay introduced by the IP network, echo is more noticeable in VoIP networks than in traditional networks. All echo cancellation algorithms require a small amount of time to adjust if the echo path changes. This results in the initial syllable, or word, of the first sentence having echo. After that, no echo is apparent.

This is a normal characteristic of the transition point between the VoIP network and traditional analog facilities. If echo is not cancelled after the beginning of the first sentence, this can be due to a more serious problem (such as impedance mismatch). Also, note that some environments, such as conference calls, can change the echo path. This also results in an adjustment period for Echo Cancellation.

Note: The source of echo on the majority of installations is incorrectly configured analog trunks. Please ensure that the trunks are configured correctly in the areas of trunk card type (EXUT/XUT), TIMP, and BIMP settings, and jumper settings on the actual trunk card itself. Also, measure the line loss and compensate using the trunk class of service NTC or TRC as required.

Nortel Networks recommends that the trunk card be an enhanced version (EXUT). An EXUT supports more complex impedance situations. Please refer to NTP 553-3001-106 for trunk cards and the NTP for your specific PBX for more information. Also, if you are connecting recording equipment or Recorded Announcement (RAN) devices to an analog trunk, ensure that the trunk impedance matches the equipment impedance to prevent echo.

Trunk options for Reach Line Cards

The following is a list of the different trunk options supported by the Reach Line Card:

- VoIP trunk
  (included through Ethernet interface)
- PRI trunk
  (clear-channel mode)

- PRI trunk
  (56K channel mode)
- T1/E1 trunk

Dial-up trunking

The RLC supports digital trunks for connections to the Remote Office units. The RLC shares the host PBX's digital trunks (ISDN PRI) for a PSTN connection to the Remote Office unit.

QoS Transitioning Technology

The RLC supports PSTN interfaces for local calling when used in Voice over IP (VoIP) mode. In this way, it also supports QoS Transitioning Technology.

For a further explanation of QoS transition functions, refer to "Adjustable QoS using QoS Transitioning Technology" on page 19. For exact configuration procedures, refer to "Configuring QoS" on page 211.

Bandwidth utilization

The voice compression algorithm that you choose when configuring DSP resources determines the bandwidth utilization of the RLC. The RLC currently supports the following compression algorithms with the Remote Office devices indicated in the table below:

The compression algorithm	uses a compressed bit rate of	on the following Remote Office devices:
G.711	64 Kbps	9150
G.726	32 Kbps	9150
G.729A	8 Kbps	911x, 9150, Meridian Digital Telephone IP Adapter

Dynamic trunk bandwidth allocation

In PSTN mode, the RLC dynamically allocates available trunk bandwidth to maximize bandwidth use. That is, as the RLC initiates calls and bandwidth requirements increase, the RLC establishes additional trunk connections for Remote Office 9150 units.

Call on-demand

The RLC supports full call on-demand (COD) functionality. This includes minimum call duration and idle timers that you can configure according to your service provider's fee structure. COD refers to the way that the RLC handles host trunk connections. In the COD mode of operation, the RLC does not establish a host connection until the user places a call to a host DN. The COD connection stays active until the minimum call duration timer expires. The RLC then closes the host connection, if idle. If another user initiates a call to the host before the timer expires, the RLC resets the timer to track the last call established. There is a single timer for each Remote Office 9150 or 911x unit.

Timers

The RLC has two timers to help manage PSTN costs.

- Minimum call duration timer

  Most PSTN tariffs specify the minimum length of time that providers can charge users for opening a connection, regardless of the call duration. This length of time determines the minimum call charges listed on long-distance telephone bills.

  Remote Office 9110, 9115, and 9150 units use the minimum call duration timer in PSTN mode only. This timer specifies the minimum length of time that each PSTN call to the host PBX remains open, regardless of telephone activity. You can configure the timer on the RLC to drop the connection just before the beginning of the next charge period, when the cost of the call increases. (Refer to Example 1 on page 26.)

- Idle timer

  Remote Office 9110, 9115, and 9150 units also use the idle timer in PSTN mode only. This timer identifies the maximum length of time a PSTN connection must remain idle before the RLC closes the connection.

An idle connection exists when no voice connections (voice paths) remain open and when no data paths exist. Users at the remote site create data paths when they press keys on their digital telephones. Signaling passing from the host PBX to the digital telephone also creates data paths.

If anyone at the remote site places another call within 60 seconds, the RLC resets the idle timer and uses the existing PSTN connection for the new call. This eliminates the need to open a new PSTN connection and incur unnecessary long distance charges. (Refer to Example 2 on page 26.)

The minimum call duration and idle timers work together to control PSTN long distance 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
After a 20-second call, the minimum call duration timer still has 39 seconds remaining. If no one else at the remote site places a call, the RLC drops the PSTN connection when the timer reaches 59 seconds. In this example, the minimum call duration timer expires before the RLC initiates the idle timer.

- After the minimum call timer, PSTN signaling with no digital telephone activity keeps the primary PSTN connection up for no longer than two idle timers.
- Every PSTN connection remains active for at least the length of the minimum call timer.
- Additional trunks and circuit-only trunks active longer than the minimum call timer remain active for an additional idle timer duration. This is the case only if no additional bandwidth requests come to the host PBX.

Example 2
After a 65-second call, the idle timer starts. If no one at the remote site places a call during the next 60 seconds, the RLC drops the PSTN connection. Since the PSTN call exceeds 59 seconds, the minimum call duration timer expires before activity ceased. At the conclusion of the call, the RLC initiates the idle timer to prevent unnecessary charges.

DN priority

The RLC provides multiple priority levels for Remote Office 9150 unit users:

- PSTN only
- high
- normal
- IP only

If you configure this feature, you must also configure an amount of bandwidth to save for the High priority DNs. You must also identify the privileged DNs through Configuration Manager. This information does not apply to Remote Office 911x series or Meridian Digital Telephone IP Adapters.

The RLC uses the *priority reserved* bandwidth for high priority DNs. When only bandwidth for *high* priority DNs remains on the network, users dialing out on *normal* priority DNs hear a fast busy signal. For details on configuring DN priority, refer to "RLC port configuration" on page 186.

Online/Offline table

You can configure the RLC to establish or terminate host connections at specified times of the day. This feature limits excessive connection charges for idle host connections. For details on configuring the Online/Offline table, refer to "Online/Offline table configuration" on page 219.

Bandwidth allocation

Configuration Manager provides options for you to allocate PSTN bandwidth for Remote Office 9150 stations. This does not apply to Remote Office 911x series or Meridian Digital Telephone IP Adapters.

- Priority reserved bandwidth

You can reserve bandwidth for certain DNs that need prioritized access to Remote Office channels. You can configure high priority DNs on the RLC Port Configuration property sheet. These DNs consume Priority Reserved Bandwidth before using unreserved bandwidth.

- Extra bandwidth

Configuration Manager allows you to reserve a certain amount of bandwidth for accessing a remote unit. When the amount of bandwidth available falls below the level that you configure, the RLC opens additional B-channels to the remote unit.

How the RLC works

When a call comes through the host PBX to a user at a remote location, the RLC makes a connection to the appropriate remote unit. The host PBX completes the call. If the RLC cannot establish a connection, the call rings until the host PBX forwards it to voice-mail.

Initiate outgoing calls by either picking up your telephone's handset or pressing a line appearance key. There are two types of appearance keys:

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

The diagrams and procedures on pages 30–34 present the details of the outgoing call process.

RLC processing modes

The RLC processes calls for a Remote Office network in one of two modes:

- host-controlled
- locally controlled

Host-controlled calls

When you place a call to someone at your host site, or when someone at your host site calls you, the call is processed in host-controlled mode. The RLC routes such calls through the host PBX. The diagrams and procedures on pages 30–33 present the details of host-controlled call processing for the Remote Office 9150 unit.

Locally controlled calls

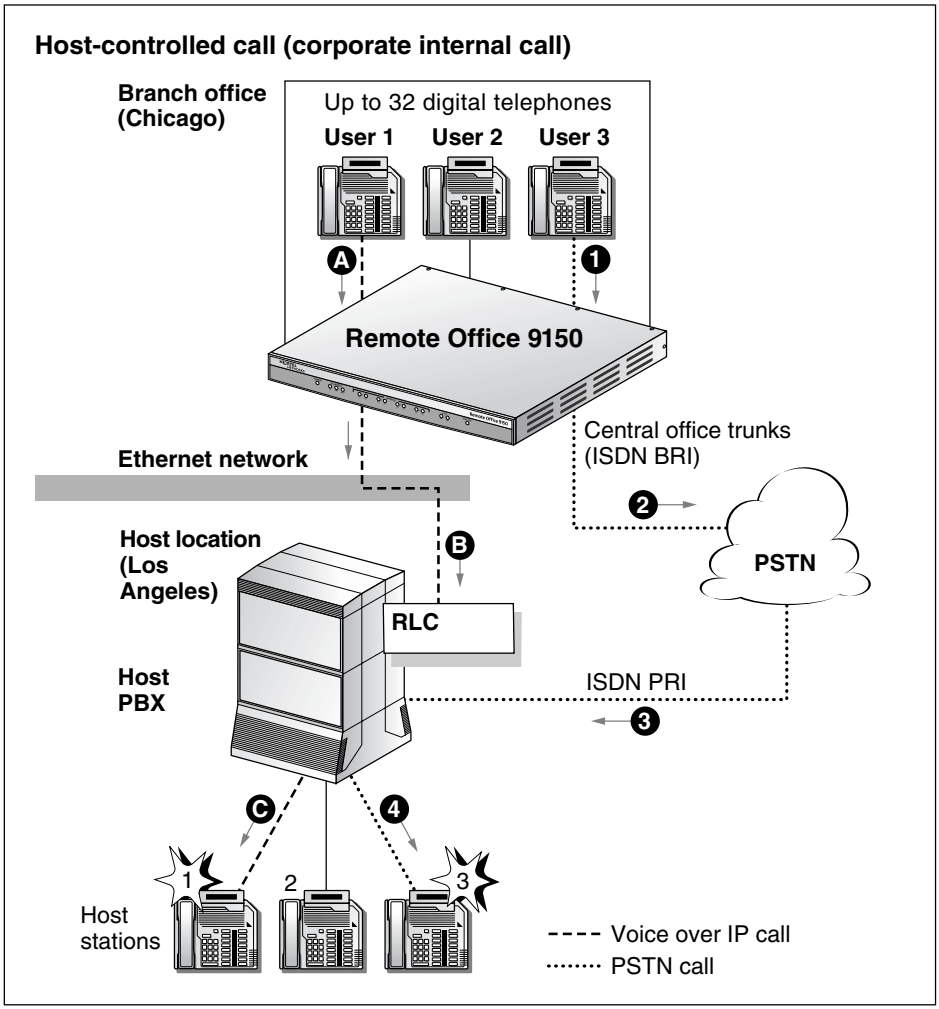
There are three types of locally controlled calls:

- A Remote Office 9150 unit user begins a call by pressing one of the local calling keys. The user then dials the DN of another local calling key. The Remote Office 9150 unit processes this call.
- A Remote Office 9150 unit user begins a call by pressing one of the local calling keys. The user then dials a local trunk access code. The local PSTN processes this call. Refer to the diagram on page 34.
- A Remote Office 911x series user begins a call by pressing a key configured as a local calling key. The user then dials a local telephone number. The local PSTN processes this call. Refer to the diagram on page 40.

The host PBX is not involved in any of the call scenarios above. These scenarios describe calls processed in the locally controlled mode.

9150 call scenario 1: host-controlled—internal corporate call

The following diagram shows how the Remote Office system routes a host-controlled call from a Remote Office 9150 unit to the corporate office.



The network that routes the host-controlled call is transparent to the user. Both VoIP and PSTN calls present the same dialing requirement, as described on page 31.

Voice over IP network call

1 Remote Office 9150 user 1 presses the host call appearance key (item A).

Result: Remote Office 9150 user 1 hears a dial tone. This indicates a successful connection to the RLC over the IP network.

2 Remote Office 9150 user 1 dials a telephone number (such as the extension number of host station 1).

Result: The Remote Office 9150 unit sends the dialed digits as packets across the Ethernet network to the RLC (item B). The RLC converts the packets to the format required by the host PBX. The host PBX then converts the data to voice and routes the call to host station 1 (item C).

PSTN call

1 Remote Office 9150 user 3 presses the host call appearance key (item 1).

Result: Remote Office 9150 user 3 hears a dial tone. This indicates a successful connection to the RLC over the PSTN.

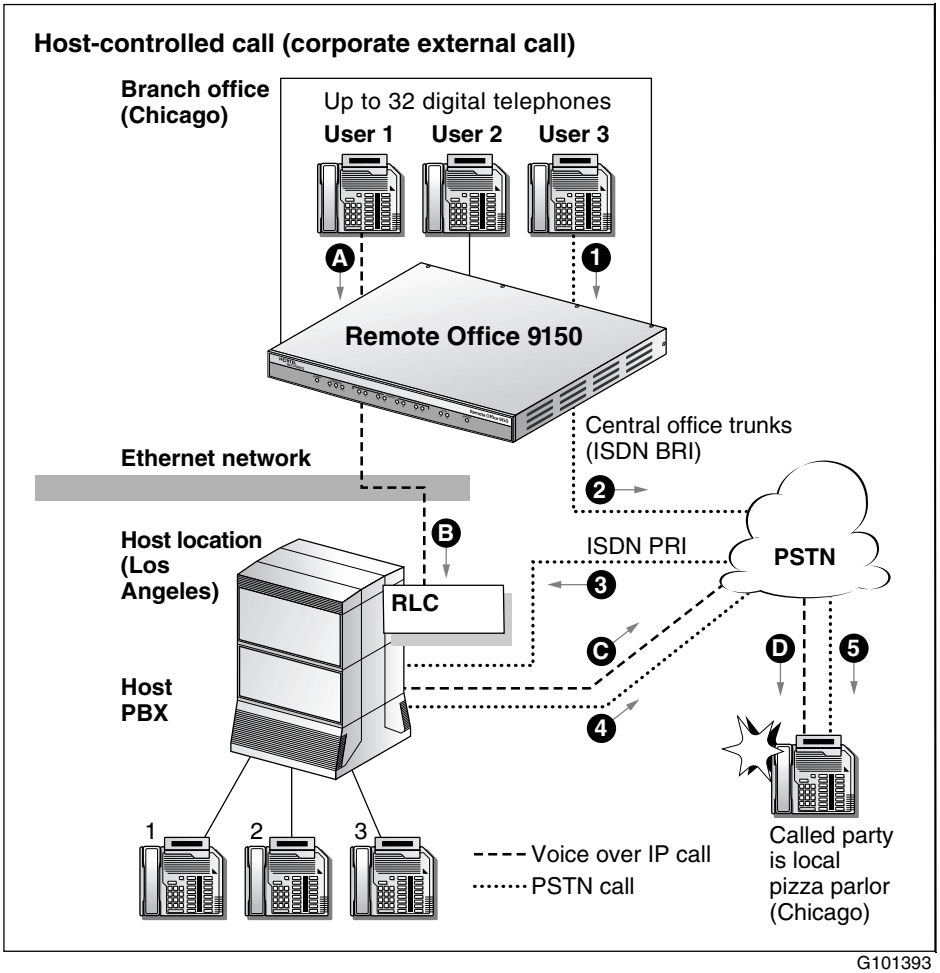
2 Remote Office 9150 user 3 dials the telephone number, such as the extension number of host station 3.

Result: The Remote Office 9150 unit sends the dialed digits across ISDN BRI through the PSTN, through the host PBX to host station 3 (items 2, 3, and 4).

Note: Item notations in parentheses refer to circled markers in the diagram on page 30.

9150 call scenario 2: host-controlled—external corporate call

The following diagram also shows how a Remote Office system routes a host-controlled call from a Remote Office 9150 unit. In 9150 call scenario 2, the call routes to a party outside the organization.



The network that routes the host-controlled call is transparent to the user. Both VoIP and PSTN calls present the same dialing requirement, as described on page 33.

Voice over IP network call

1 Remote Office 9150 user 1 presses the host call appearance key (item A).

Result: Remote Office 9150 user 1 hears a dial tone. This indicates a successful connection to the RLC over the IP network (item B).

2 Remote Office 9150 user 1 dials the external telephone number.

Result: The Remote Office 9150 unit sends the dialed digits as packets across the Ethernet network. The RLC converts the packets to the format required by the host PBX. The host PBX then converts the data to voice and routes the call through the PSTN to the called party (items C and D).

PSTN call

1 Remote Office 9150 user 3 presses the host call appearance key (item 1).

Result: Remote Office 9150 user 3 hears a dial tone. This indicates a successful connection to the RLC over the PSTN (items 2 and 3).

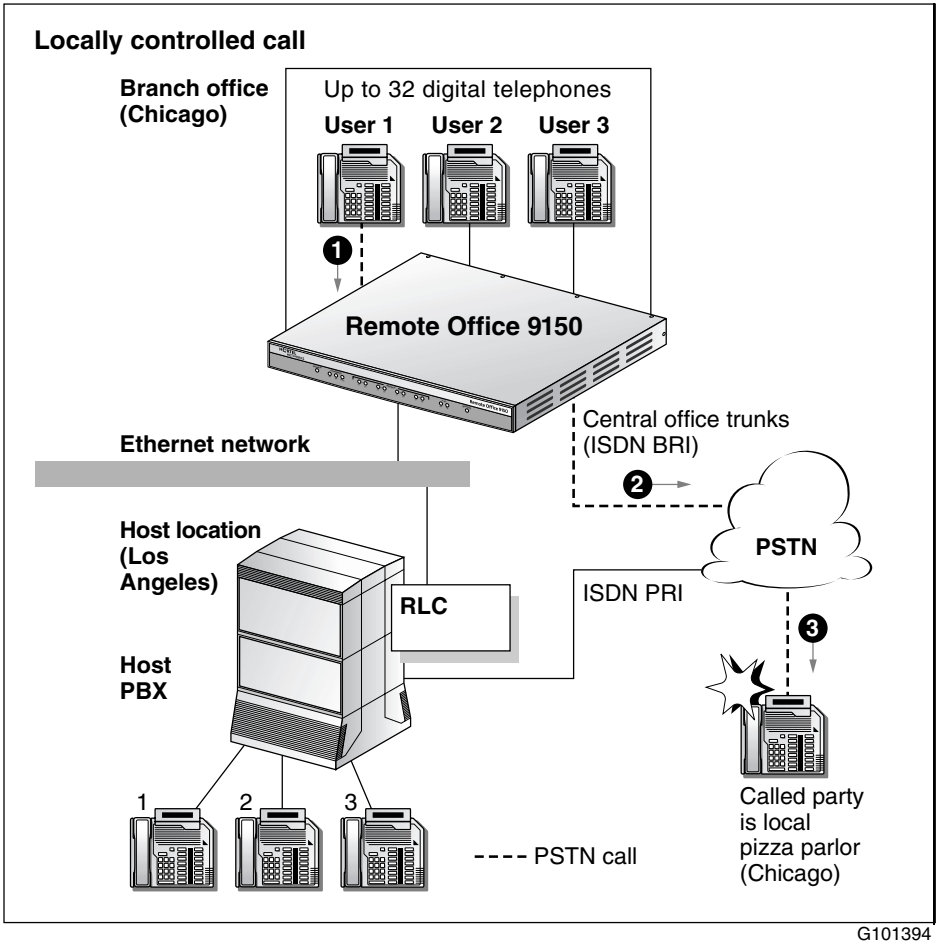
2 Remote Office 9150 user 3 dials the external telephone number.

Result: The Remote Office 9150 unit sends the dialed digits across ISDN BRI through the PSTN, through the host PBX to the called party (items 4 and 5).

Note: Item notations in parentheses refer to circled markers in the diagram on page 32.

9150 call scenario 3: locally controlled—local call

The following diagram shows how a Remote Office system routes a call within your local area.



Local call

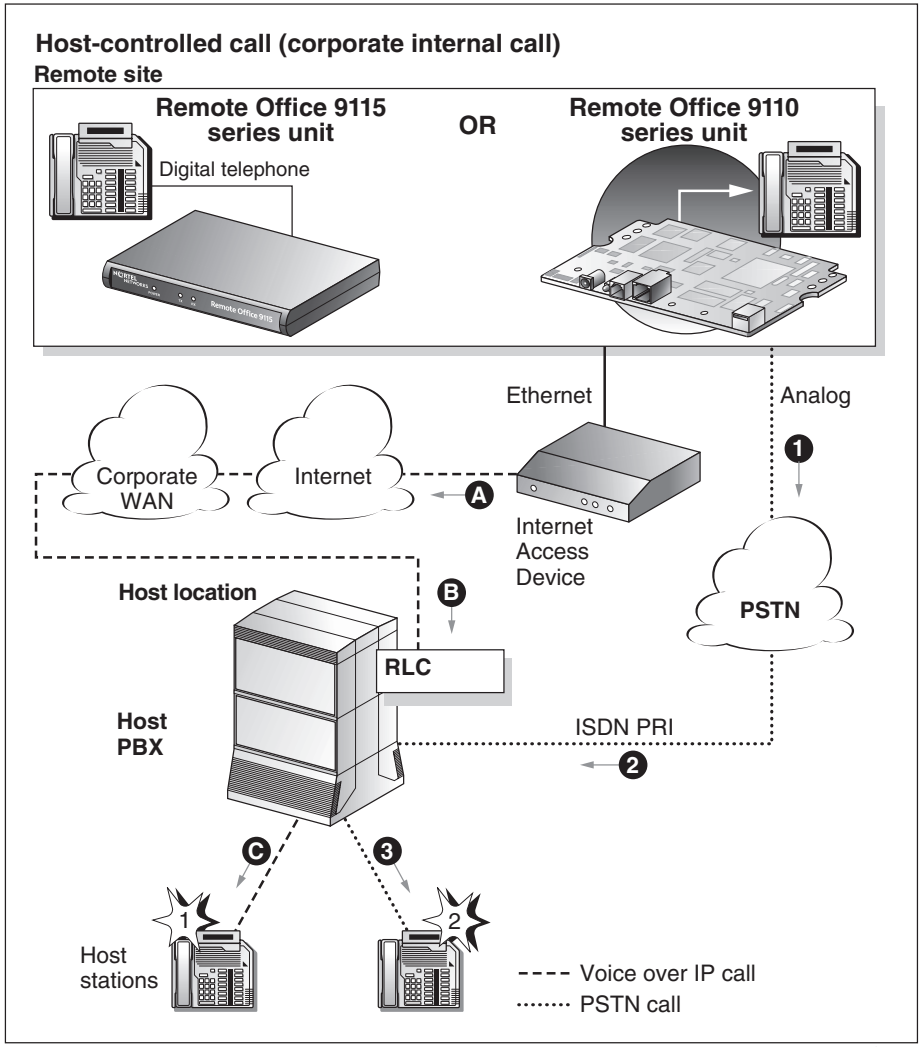
1. Remote Office 9150 User 1 presses the local call appearance key and hears a dial tone from the Remote Office 9150 unit (item 1).
2. Remote Office 9150 User 1 then dials a trunk access code and hears a PSTN dial tone from the Central Office (item 2).
3. Remote Office 9150 User 1 dials the telephone number (the pizza parlor in this example). The dialed digits travel across the ISDN BRI connection through the PSTN to the called party (item 3).

Note: Item notations in parentheses refer to circled markers in the diagram on page 34.

For details about how the Remote Office system routes calls from Remote Office 911x series units, refer to pages 36 through 40.

911x call scenario 1: host-controlled—internal corporate call

The following diagram shows how the Remote Office system routes a host-controlled call from a Remote Office 911x unit to the corporate office.



The network that routes the host-controlled call is transparent to the user. Both VoIP and PSTN calls present the same dialing requirement, as described on page 37.

Voice over IP network call

1 The Remote Office 911x user lifts the handset (item A).

Result: The Remote Office 911x user hears a dial tone. This indicates a successful connection to the RLC over the IP network (item B).

2 The Remote Office 911x user dials a telephone number, such as the extension number of host station 1.

Result: The Remote Office 911x unit sends the dialed digits as packets through the IP network to the Ethernet network or Corporate WAN to the RLC. The RLC converts the packets to the format required by the host PBX.

3 The host PBX then converts the data to voice and routes the call to host station 1 (item C).

PSTN call

1 The Remote Office 911x user lifts the handset.

Result: The Remote Office 911x user hears a dial tone. This indicates a successful connection to the RLC over the PSTN (item 1).

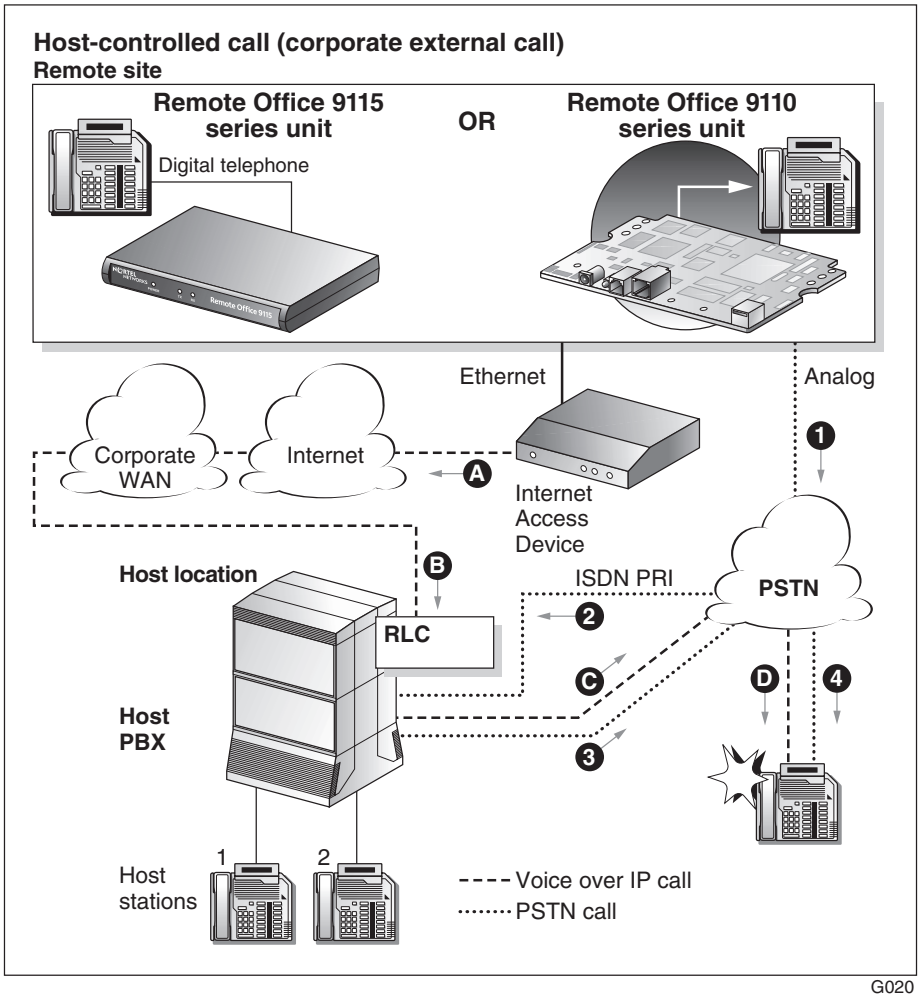
2 The Remote Office 911x user dials a telephone number, such as the extension number of host station 2.

Result: The Remote Office 911x unit sends the dialed digits across the PSTN through the host PBX (item 2) to host station 2 (item 3).

Note: Item notations in parentheses refer to circled markers in the diagram on page 36.

911x call scenario 2: host-controlled—external corporate call

The following diagram also shows how a Remote Office system routes a host-controlled call from a Remote Office 911x series unit. In 911x call scenario 2, the call routes to a party outside the organization.



The network that routes the host-controlled call is transparent to the user. Both VoIP and PSTN calls present the same dialing requirement, as described on page 39.

Voice over IP network call

1 The Remote Office 911x user lifts the handset (item A).

Result: The Remote Office 911x user hears a dial tone. This indicates a successful connection to the RLC over the IP network and the corporate WAN (item B).

2 The Remote Office 911x user dials the external telephone number.

Result: The Remote Office 911x series unit sends the dialed digits as packets across the Ethernet network. The packets go through the IP network and the corporate WAN, to the RLC. The RLC converts the packets to the format required by the host PBX. The host PBX then converts the data to voice and routes the call through the PSTN to the called party (items C and D).

PSTN call

1 The Remote Office 911x user lifts the handset (item 1).

Result: The Remote Office 911x user hears a dial tone. This indicates a successful connection to the host PBX over the PSTN (item 2).

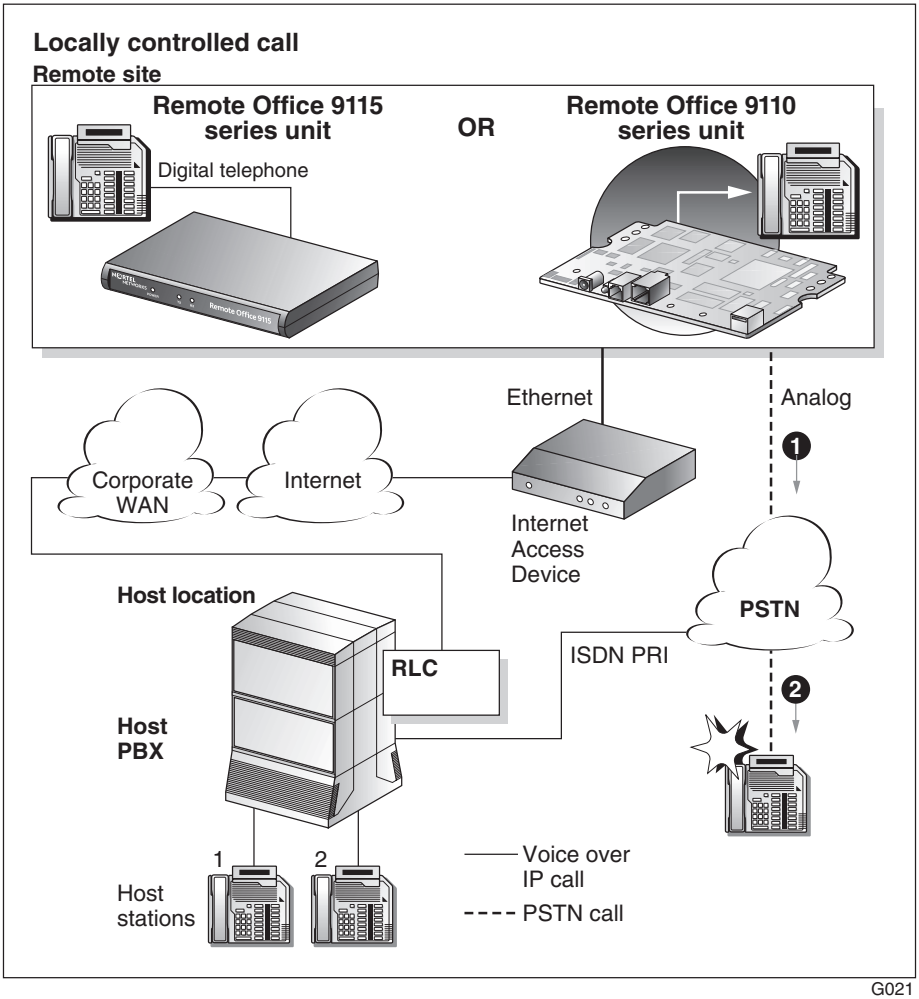
2 The Remote Office 911x user dials the external telephone number.

Result: The Remote Office 911x series unit sends the dialed digits across an analog line through the PSTN, through the host PBX to the called party (items 3 and 4).

Note: Item notations in parentheses refer to circled markers in the diagram on page 38.

911x call scenario 3: locally controlled—local call

The diagram below shows how a call is routed when placing a call within your local area using a Remote Office 911x series unit.



Local call

1 Do the following:

IF the Remote Office 911x unit is	THEN the Remote Office 911x user
offline, or not connected to the host PBX,	lifts the handset.
online, or connected to the host PBX,	presses the local calling key

Result: The Remote Office 911x user hears a PSTN dial tone from the Central Office (item 1).

2 The Remote Office 911x user dials the external telephone number.

3 The dialed digits travel across the PSTN to the called party (item 2).

Note: Item notations in parentheses refer to circled markers in the diagram on page 40.

Environmental requirements

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

Specification	Minimum	Maximum
Operating temperature		
Normal (Ambient)	0°C (32°F)	60°C (140°F)
Operating humidity		
Normal	5% (noncondensing)	95% (noncondensing)
Storage		
Recommended temperature	-40°C (-40°F)	70°C (158°F)
Relative humidity	5% RH (noncondensing)	95% RH (noncondensing)

Power requirements

This section lists characteristics of the recommended power supplies for the Remote Office 9150 unit, the Remote Office 911x series units, and the Meridian Digital Telephone IP Adapter units.

9150 units

Input specifications for the Remote Office 9150 unit are as follows:

Characteristics	Rating
voltage	85 - 264 VAC
frequency	47 - 63 Hz
current	3.20A maximum, 115 VAC (North American installations) 1.80A maximum 230 VAC (non-North American installations)

Output specifications for the Remote Office 9150 unit are as follows:

Characteristic	Rating
Output 1 voltage	5VDC +/-5%
Output 1 current	10.0A maximum
Output 2 voltage	24VDC +/-5%
Output 2 current	3.0A maximum
maximum power	110W

Remote Office 911x series and Meridian Digital Telephone IP Adapter units

Input specifications for the Remote Office 911x series units, including the Meridian Digital Telephone IP Adapter units, are as follows:

Characteristic	Rating
voltage	90 - 264 VAC
frequency	47 - 63 Hz
current	0.4A maximum

Output specifications for the Remote Office 911x series units, including the Meridian Digital Telephone IP Adapter units, are as follows:

Characteristic	Rating
voltage	24 VDC +/-5%
current	0.62A maximum
power	15W maximum

Administration software

Configuration and administration of the RLC is performed with Remote Office 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 obtain the CD from your Nortel Networks distributor or click on the **Software Downloads** link at the following website:

www.nortelnetworks.com

Administration PC connection options

You can connect the administration PC to the RLC through the following:

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

Remote Office Configuration Manager

Remote Office Configuration Manager allows you to configure the RLC. It also provides the Configuration Wizard for first-time configuration. The Configuration Wizard prompts you for the minimum information that is needed to get the RLC communicating with the RLC on the host PBX. After the initial configuration is completed, use Configuration Manager to administer the RLC. Administration tasks include the following:

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

Note: Configuration Manager alerts you when you must restart after you have made a configuration change.

Command line interface

When the administration PC is connected to the RLC 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. Only use the command line interface with the assistance of technical support personnel for troubleshooting and diagnostic testing. Configuration Manager is the supported tool for customer administration of the RLC over both the serial port and Ethernet connections. For further information, refer to “What is Configuration Manager?” on page 126.

Chapter 2

Planning for RLC installation

In this chapter

Preinstallation preparation

To prepare a site for installation, consider the environment, structural and electrical factors, and other site-specific limitations. For more information on site-preparation from an equipment standpoint, refer to the following documents:

- *Small System Planning and Engineering* (NTP 553-3011-120)
- *Large System Planning and Engineering* (NTP 553-3021-120)
- *Communication Server 2100 (CS 2100) Intelligent Peripheral Equipment-IPE* (NTP 555-4001-129)
- *Communication Server 1000 (CS 1000) Planning and Engineering* (NTP 553-3031-120)

Planning for your remote service needs

Plan for your remote service needs by determining the total number of simultaneous remote service telephone calls you want to support on your network. This number tells you how many RLC ports that you need.

RLC requirements

Once you have determined the total number of RLC ports that you need in your remote service network, you can determine the number and size of RLCs needed at your host site.

Every 16 remote service ports in your network requires one card slot in the host PBX and 16 ports on an RLC. If you want your network to support more than 16 remote service ports, you need at least one 32-port RLC.

The following table gives a summary of how to choose the correct size RLC for your specific remote service needs.

IF the number of remote-service ports in your network is	THEN you need
under 17,	a 16-port RLC.
between 17 and 32,	a 32-port RLC.
over 32,	to consult with your Nortel Networks distributor to determine the most cost-effective combination of 16- and 32-port RLCs.

DSP requirements

The total number of simultaneous telephone calls that you want to support also determines the number of DSP application modules that you need.

- Both 16- and 32-port RLCs come equipped with enough built-in DSP resources to provide non-blocking service for up to 8 simultaneous calls.
- Each remote telephone call to the host PBX requires one DSP channel.
- Each DSP application module has eight channels that provide eight additional voice paths between host and remote sites.

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

1. The basic 16-port RLC ships with eight built-in DSP channels. With no hardware changes, the 16-port RLC supports up to 16 users, allowing up to eight simultaneous calls.
2. When you add one DSP application module to the 16-port RLC, the line card now holds 16 DSP channels. This combination supports up to 16 users, allowing up to 16 simultaneous calls.
3. The basic 32-port RLC ships with eight built-in DSP channels. With no hardware changes, the 32-port RLC supports up to 32 users, allowing up to eight simultaneous calls.

4. When you add three DSP application modules to the 32-port RLC, the line card has 32 DSP channels. This combination supports up to 32 users, allowing up to 32 simultaneous calls.

Note: When you add data channel adapters (MCAs and ATAs) to a remote site, that site's DSP channel usage increases. Every remote call, whether from a telephone, MCA, or ATA, requires a DSP channel.

Each DSP device configured with the 911x DSP load supports up to four modem channels.

Installation planning

Make an outline of cable routing between the I/O panel of the shelf where the RLC resides and the following components of your Remote Office system:

- your PBX's serial port
- the I/O-panel connection to the IOP (input-output port) card for access to your PBX's internal Ethernet, or ELAN
- the cross-connect device to the local telephones using the RLC ports not providing remote services

Note: The RLC operates properly without the last two connections listed above. These two connections are available only with the RLC Multi-I/O cable–Enhanced. Refer to page 12 for more information on this cable.

Deployment planning

Include the configuration settings for each station at each remote site and for each port at the host site in your deployment plan. Use Appendix A, "Planning forms", on page 325 to help with this task.

Before you can configure the system with Configuration Manager, you must configure PBX voice and data ports for each RLC port. Refer to "Configuring remote and network ports" on page 111.

Checklists

Use the RLC Installation Checklist on page 52 as a guide to ensure complete RLC installation and configuration.

Planning forms

Appendix A, “Planning forms”, contains the following forms for you to record and store your configuration plans:

- Connection Information—16 ports
- Connection Information—32 ports
- Online/Offline Table Configuration
- System expansion worksheet

Refer to “Related information products” on page xxiv for information on accessing these forms online.

Taking inventory

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

Installation checklist

When you are preparing to install your Meridian system, use the checklist on following pages to ensure that you complete all the required processes properly.

RLC Installation Checklist

Page 1 of 7

Use this checklist to ensure completion of all installation tasks.

✔	Task	For details, refer to
1. Planning		
❒	Check the Remote Office web site for the latest Release Notes with last-minute product updates.	the *Remote Office and RLC Release Notes* (NTP 555-8421-102) at the following address: **www.nortelnetworks.com**
❒	Ensure that you have the latest firmware and software.	the *Remote Office and RLC Release Notes* (NTP 555-8421-102). This document ships with Remote Office equipment. You can obtain additional copies online at the following address: **www.nortelnetworks.com**
❒	Ensure that your PBX platform and software release support the RLC.	"PBX hardware and software compatibility".
❒	Ensure that a slot is available on the PBX IPE shelf or Meridian 1 PBX 11 cabinet for each RLC. Order additional shelves if necessary.	your Nortel Networks distributor.
❒	To route calls over the IP network, the PSTN, or both, determine what you must do to implement these call routing methods.	"Deployment options".

RLC Installation Checklist

Page 2 of 7

✔	Task	For details, refer to
❒	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 ■ the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103) You can obtain this document online at the following address: **www.nortelnetworks.com**
❒	Plan the installation and cabling of RLCs.	Chapter 2, “Planning for installation”.
❒	Decide on the administration PC setup.	“Administration PC”.
❒	Obtain the cables that you need to establish the needed connections to the network.	“Reach Line Card cables”.
❒	Gather the configuration information (network addresses, connection numbers, online/offline schedule, QoS thresholds, and so on).	■ “Deployment options” ■ Appendix A, “Planning forms”
❒	Plan RLC port assignments.	“Connection Information—16 ports” or “Connection Information—32 ports”, depending on your RLC.

RLC Installation Checklist

Page 3 of 7

✔	Task	For details, refer to
2. PBX configuration		
❒	Configure the PBX to recognize each RLC as an XDLC.	documentation for your PBX.
❒	Verify that the PBX recognizes each RLC as an XDLC.	
❒	If you want to use the PSTN to route calls, ensure that ISDN BRI or PRI trunks are installed and configured on the PBX for voice and data.	configuration on your PBX.
❒	Ensure that there is sufficient capacity on the trunks for the extra traffic involved in remote service operations.	configuration on your PBX and the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103). You can obtain this document online at the following address: **www.nortelnetworks.com**
❒	Configure a voice port (or data port for MCA) on the PBX for each remote user. (These ports are associated with Remote ports on the RLC.)	documentation for your PBX.
❒	Configure a data port (or voice port for 911x modem) on the PBX for each remote unit connection. (These ports are associated with Network ports on the RLC.)	

RLC Installation Checklist

Page 4 of 7

✔	Task	For details, refer to
3. Hardware and software installation		
❒	Install DSP application modules on the RLC, if required.	"Installing DSP application modules".
❒	Install and cable each RLC.	■ "To install an RLC" ■ "To cable an RLC"
❒	Install the software from the product CD-ROM or download the software from the Nortel Networks web site.	"Installing the software".
4. RLC configuration		
❒	Configure the IP address, subnet mask, and default gateway on the RLC.	"Using the Configuration Wizard to perform initial configuration".
❒	If you want to use the PBX's administration terminal to administer the RLC, configure the IP address and subnet mask of the RLC's ELAN port.	"IP Configuration".
❒	Configure the following items, as required, to create the communication paths between the RLC and the remote unit: ■ IP network: remote unit's IP address ■ PSTN: remote unit's telephone number ■ security level and, if required, security identifier	■ "Using the Configuration Wizard to perform initial configuration" ■ "To configure remote connection settings"

RLC Installation Checklist

Page 5 of 7

✔	Task	For details, refer to
❒	Configure a Remote port on the RLC for each user. **Note:** The process of creating the PSTN communication path with the Configuration Wizard creates a Network port for each remote unit.	Chapter 6, “Configuring the Reach Line Card”.
❒	Configure an Online/Offline Schedule for each remote unit, if required.	“Configuring an online/offline table”. **Note:** A blank online/offline schedule can be found in the Online/Offline Table section of Configuration Manger.
5. Remote unit configuration		
❒	Ensure that the remote unit is configured with the information it needs to establish connections with the RLC.	the *Installation and Administration Guide* for the remote unit.
❒	Ensure that a station is configured for each remote user.	the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215), or the *Remote Office 911x Series Installation and Administration Guide* (NTP 555-8421-220), depending on remote site equipment.

RLC Installation Checklist

Page 6 of 7

✔	Task	For details, refer to
6. Network configuration		
❒	Configure network devices ■ so that voice traffic is not constrained or congested ■ to maximize network efficiency for Voice over IP service	■ your data network administrator ■ the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103) You can obtain this document online at the following address: **www.nortelnetworks.com**
	Ensure that voice calls can be sent or received over the following:	■ your data network administrator
❒	■ IP network	■ your telecom network administrator
❒	■ PSTN	
❒	Ensure that processing of voice and data traffic over the IP network performs as expected.	■ your data network administrator ■ your telecom network administrator ■ the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103) You can obtain this document online at the following address: **www.nortelnetworks.com**
❒	Adjust QoS transitioning settings, if required.	

RLC Installation Checklist

Page 7 of 7

✔	Task	For details, refer to
7. Testing		
❒	PING the RLC to ensure that it is recognized as a device on the network.	"Testing the connections".
❒	Ensure that calls can be made and received on each RLC port.	"Testing the connections".
8. Administration		
❒	Plan for administration training and technical support.	■ Chapter 7, "Administration" ■ Chapter 8, "Troubleshooting"

Note: The RLC and Configuration Manager software are Year 2000 compliant.

System resources management

The RLC offers the following methods to manage system resources:

- QoS Transitioning Technology
- Host connection management
  - — Configurable trunk connection accessibility (permanent or on-demand)
  - — Call timers for managing of on-demand trunks
- Online/offline scheduling
- Configurable security

QoS Transitioning Technology

Traffic congestion often results in poor voice quality or lost connections on IP networks. For a description of the RLC's QoS Transitioning Technology, refer to "Adjustable QoS using QoS Transitioning Technology" on page 19.

For detailed information on configuring QoS Transitioning Technology thresholds, refer to "Configuring QoS" on page 211.

Host connection management

Manage connections to the host PBX in the following three ways:

- Configure an Online/Offline table for the remote site to determine when it can and cannot place or receive calls through the host PBX.
- Define a trunk connection as permanent or on-demand so that it is one of the following:
  - — Always connected (permanent)
  - — Connected when bandwidth required (on-demand)
- Define minimum call duration and idle timers to address call-establishment and PSTN charges, if the trunk connection is defined as on-demand.

Call-on-demand

The RLC supports full call-on-demand (COD) capability. In COD mode, the RLC does not establish a connection to the remote site until the remote unit places a call to a host DN. For further information on the RLC's COD functionality, refer to "Call on-demand" on page 25.

Online/offline schedule

You can configure an online/offline schedule on the RLC to control when remote sites can place and receive calls through the host PBX.

Note: Online/offline schedules configured for Remote Office 9150 units affect all users connected to that unit.

Configure offline entries for the following situations:

- to restrict remote users from placing or receiving calls at certain times, such as during evenings and weekends
- to eliminate unwanted telephone access charges by preventing remote sites from staying online permanently

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

For example, suppose you configure an offline entry for 6:00 p.m. and the next online entry for 9:00 a.m. the next day. When the RLC processes the 6:00 p.m. entry, it instructs the remote site to go offline for 15 hours.

When going offline, the system activates a timer at the remote site. When the timer expires (in the example above, at 9:00 a.m.), the remote site initiates a "going online" request to the host PBX. If the RLC successfully receives the request, the remote site and its telephones go online.

Changing the online/offline mode

You can put the remote site into online or offline mode at any time. Simply dial one of two special prefix (SPRE) codes at any remote site telephone set. Configure the online SPRE and offline SPRE codes through Configuration Manager. These codes must not conflict with the dialing plans used at the host PBX. Refer to "9150 System Configuration" in the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215), for information on configuring SPRE codes.

Configurable security

Security settings apply to the RLC on a remote unit basis. Enter this information through Configuration Manager. Refer to "Remote connection configuration" on page 197.

The RLC offers three levels of security. For a detailed description of the RLC's variable the security levels, refer to "Multiple security levels" on page 21.

Data network security

The RLC does not provide for data network security. To provide security on the data network, implement security on the data network devices.

System security

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

- Local password

  You must enter the local password when starting Configuration Manager software. If the person attempting to use Configuration Manager does not have the password, the Remote Office system blocks that person from accessing any Remote Office nodes.

- Node password

  Users must enter the node password before Configuration Manager displays the configuration of the logged-on node and allows modification of that configuration.

ATTENTION!

Nortel Networks recommends that users retain the factory-set password until the system is up and running smoothly.

Lost or forgotten passwords

If you lose or forget your RLC or Configuration Manager password, contact your Nortel Networks supplier for assistance.

Network considerations

When you implement an RLC-based remote service system, consider the ways that the new equipment effects your current telecommunications and data networks.

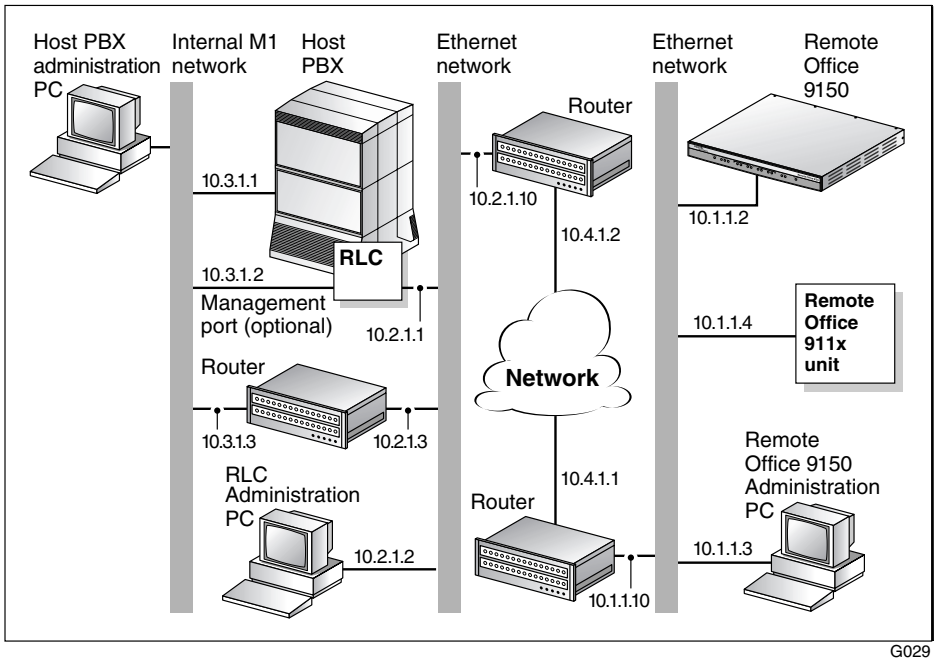
IP addressing and routing

To place and receive calls over the IP network, the RLC must have:

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

Network diagram

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



QoS

The routers used on your IP network must handle voice traffic while introducing little or no congestion and few delays into the network. Network congestion or excessive delay adversely effects voice quality.

Impact of delay on voice quality

The impact of the different voice algorithms (G.729A, G.726, and G.711) is well documented. G.729A provides 8 to 1 compression and does not produce perfect voice quality. Most users consider it quite acceptable, although some users claim that they can hear the difference between it and G.711. The 8 to 1 compression ratio and the acceptable voice quality make it the codec of choice for Voice over IP (VoIP). Multiple instances of transcoding (that is, compressing and decompressing) can have a significant impact on voice quality. G.729A is more likely to be negatively affected by transcoding than G.711.

Most users do not understand the impact of network/PSTN delay or the impact of voice compression algorithms on the perceived quality of voice. In order to compensate for the variation in transmission time across the network (IP and PSTN), the Meridian product uses a jitter buffer to allow voice packets to pass through it in a constant stream. The purpose of the jitter buffer is to remove the variable delays from the voice packets sent across the network, thus avoiding awkward-sounding speech. The default value of this jitter buffer is 90 milliseconds (ms).

Note: Once you configure the jitter buffer, the jitter buffer can vary up to 30 ms above or below the configured target.

To estimate the total delay the user experiences, add the following values:

- jitter buffer delay
- network delay
- algorithmic encoding delay of the algorithm in use

To make the calculation simple, use 30 ms as the algorithmic delay. (It varies depending on the voice algorithm, but 30 ms is a good estimate).

The following table indicates one-way delay in ms for the common configurations. It can seem unusual that the ISDN delay is larger than the IP delay. However, this is due to the serialization delay of sending the packets across the relatively low-speed (64K) channels provided by ISDN. (The IP Network delay assumes high-speed Internet access as part of the intranet.)

	IP Network Delay	G.729A Over PSTN	G.726 Over PSTN	G.711 Over PSTN
Minimum *recommended* jitter buffer setting	30	30	60	90
Algorithmic delay	30	30	30	30
Reasonable network delay	10	20	20	20
Total One Way Delay	70	80	110	140

Excessive delay results in users talking over each other (that is, both users speaking at the same time). Studies vary as to when this becomes a voice quality problem, but most of them suggest that this occurs between 120 and 180 ms.

Real-time data transmission produces two types of packet loss:

- network-related packet loss (that is, packets lost due to either errors or delays in transmission)
- jitter buffer-related packet loss (that is, packets lost due to their being thrown away when the jitter buffer is full)

In effect, there is a trade-off between jitter buffer delay (jitter buffer size) and packet loss delay at the Remote Office unit. The relationship between jitter buffer size and packet loss has a direct impact on the user's perception of voice quality.

Customer feedback and experience indicate that configuring the jitter buffer to reduce delay produces better results. Delay, as introduced by the size of the jitter buffer, is inversely proportional to lost packets. A jitter buffer configuration of 30 ms results in less delay, but a greater likelihood of lost (thrown away) packets. Most customers find packet loss of 1% far more acceptable than an increase in one-way delay beyond 180 ms.

Trunks and dialing plans

To obtain an outside line on the local PSTN, users dial local trunk-access SPRE codes. The SPRE codes configured for remote sites must not conflict with the dialing plans used by the host PBX. Conflicts result in end-users not being able to place outgoing calls through the local PSTN.

Call blocking

The voice processing capacity of a remote system depends on the number of DSP application and trunk interface modules installed at the host and remote sites. Voice processing capacity defines the number of calls that can be active simultaneously and the amount of bandwidth the site can access.

Reducing call blocking in PSTN mode

Remote Office 9150 units use ISDN BRI trunks in PSTN mode. To reduce call blocking in the PSTN mode at the host location, you must increase the number of trunks available to the RLC.

Reducing call blocking in Voice over IP mode

One DSP application module provides the ability to support eight simultaneous Remote Office calls. To reduce call blocking for Voice over Internet Protocol (VoIP) calls, increase the number of DSP resources in your system. Do this at the host (RLC) site and, if the remote unit is a Remote Office 9150 unit, at the remote site. You can install up to four DSP application modules on a Remote Office 9150 unit and up to four DSP application modules on an RLC.

Calculating system requirements

For help in determining how many DSP application modules you need to install to reduce or eliminate call blocking, refer to “DSP requirements” on page 49 and the RLC System expansion worksheet on page 343.

Administration PC

Install the Windows-based RLC administration software on a PC in the Remote Office network. This section describes options for connecting an administration PC to the RLC. It also describes the hardware and software requirements of the administration software.

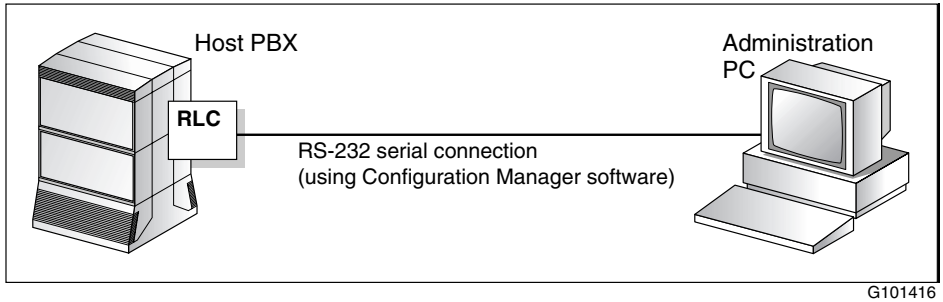
Connection options

The RLC product includes the Configuration Manager software that enables you to configure, administer, and upgrade the RLC. Perform these tasks over one of the following connections:

- RS-232 serial connection
- 10BaseT Ethernet connection

Serial connection

Use the serial connection when you first install and configure the RLC. You must establish a serial connection to the RLC to enter the IP interface information. Refer to the following illustration:

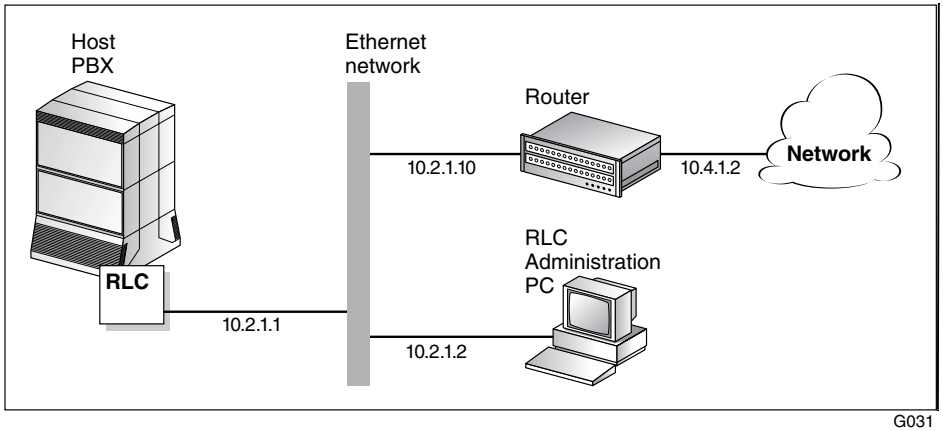


You can continue using the serial connection for ongoing administration of the RLC if you prefer.

Ethernet connection

Configure the RLC's IP interface information to allow calls to be routed between the RLC and remote units. This also allows RLC administration to take place over the IP network from a remote location.

Remote administration of the RLC means you can install the administration PC in a location different from that of the RLC. Refer to the following illustration:



Administering multiple nodes

If you are responsible for administering the RLC on the host PBX and one or more remote units, you can access the RLC and the remote unit from anywhere on the network.

Windows PC requirements

To use Configuration Manager, the administration PC must:

- be an IBM-compatible PC
- use a Windows 95, 98, NT Workstation 4.0, Millennium Edition (ME), 2000 Professional, or XP (Professional and Home Edition) operating system with the Microsoft TCP/IP networking component installed
- be equipped with a CD-ROM drive
- be equipped with a 10BaseT Ethernet interface card
- 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, such as a mouse
- use Microsoft's IP stack
- have 32 Mbytes of RAM for Windows 95, 98, and ME, or 64 Mbytes of RAM for Windows NT Workstation 4.0, 2000 Professional, and XP (Professional and Home Edition
- have 48 Mbytes of available storage for Windows 95, 98 and ME, or 64 Mbytes of available storage for Windows NT Workstation 4.0, 2000 Professional, and XP (Professional and Home Edition)

Note: Configuration Manager does not support any of the Win32 Server versions of Microsoft Windows.

Trivial File Transfer Protocol (TFTP) server

Firmware upgrades and configuration uploads require that the administration PC have a TFTP server application installed. The administrator must know the TFTP server's IP address in the network. In other words, the IP address of the administration PC.

You can use any TFTP server application. These applications are available free of charge on the Internet.

Year 2000 compliance

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

Operating system	Year 2000 compliance requirement
Windows 95	Version 95b
Windows 98	OK as is
Windows NT Workstation 4.0	Service Pack 5 or higher
Windows 2000	Ok as is
Windows ME	Ok as is
Windows XP	OK as is

Optivity Telephony Manager and Configuration Manager

Nortel Networks does not guarantee that Optivity Telephony Manager (OTM) and the Configuration Manager can operate simultaneously on the same administration PC. Simultaneous running of these two applications has not been tested and is, therefore, not supported.

Planning for future growth

The RLC can change as your telecommunication needs change or grow. When determining remote port needs for your network, it is important to consider the number of users and estimated growth at each site in the network.

Adding DSP modules

The RLC ships with enough built-in DSP resources to support up to eight simultaneous telephone calls without the addition of any DSP application modules. For information on increasing the voice processing capability of the RLC, refer to “DSP requirements” on page 49.

For help determining how many DSP application modules you need to meet your call-processing expectations, refer to the “System expansion worksheet” on page 343. For instructions on installing additional DSP modules, refer to “Installing DSP application modules” on page 81.

Deployment options

You can install and configure the RLC on the host PBX and remote units at remote sites with the following network capabilities:

- only the IP network (Voice over IP)
- only the PSTN (for example, ISDN BRI trunks)
- both networks (required for QoS Transitioning Technology functionality)

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

ATTENTION!

Even if you plan to route calls over the PSTN only, you must assign an IP address and IP gateway to the RLC and remote units to allow remote administration.

Port and station assignment

Regardless of which network you use initially to route calls, you must plan RLC port and remote site user station assignments. Assign a single user to each RLC port, unless you are using the RLC's port sharing functionality (refer to "Port sharing options" on page 20). Use the following forms to plan port and station assignment:

- "Reach Line Card Connection Information—16 ports" on page 328
- "Reach Line Card Connection Information—32 ports" on page 333

Implementing PSTN mode

In a scenario involving the PSTN mode only, the PSTN processes all incoming and outgoing calls as follows:

IF the call is to or from the	THEN the call is in
host PBX,	host-controlled mode.
other PSTN customers,	local-controlled mode.

To implement PSTN mode, you must complete the following steps:

1. Determine how many simultaneous calls you want to process over the PSTN.

   Note: Include all single-user Remote Office 911x series and Meridian Digital Telephone IP Adapter sites along with all multi-user Remote Office 9150 sites that use the same RLC in this calculation.

   If the remote unit is a Remote Office 911x series unit, configure the appropriate number of DSP resources on the RLC for 911x use. For the necessary procedure, refer to Chapter 6.

2. Arrange for PSTN lines to each remote site if these lines are not already present.

3. Install up to four DSP application modules on the RLC to increase voice processing capability if needed.

   Note: RLCs do not ship with DSP application modules installed.

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

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

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

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

Note: For Remote Office 9150 units, remember to get this information for each ISDN BRI line.

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

Implementing Voice over IP mode

In Voice over IP (VoIP) mode, the system processes all incoming and outgoing calls across the IP network through the host PBX. The system routes calls made to external parties to the PSTN using host PBX trunks. Calls processed through the host PBX are referred to as *host-controlled calls*.

Note: Local PSTN calls at Remote Office 9150 sites require access to ISDN BRI lines and the installation of ISDN BRI application modules in the Remote Office 9150 unit. Local PSTN calls made at Remote Office 9110 and Remote Office 9115 sites use analog, POTS lines. All calls not routed through the host PBX, whether ISDN or POTS, are referred to as *locally controlled calls.*

To implement VoIP mode for host-controlled calls:

1 Determine how many simultaneous calls you want to process. This helps you to determine how many DSP application modules to install on the RLC. To do this, complete the RLC System expansion worksheet on page 343.

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

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

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

5 Run this stage with a small number of users at first. Before applying VoIP mode to your entire remote network, you must ensure that one of the following is true:

- Your IP network can handle the addition of remote network traffic.
- You can identify the kinds of configuration adjustments you need to make to the IP network so that it can handle the additional traffic.

When you are satisfied with the IP network performance, continue with QoS Transitioning Technology implementation.

Implementing QoS Transitioning Technology

To implement the QoS Transitioning Technology, you must understand characteristics of your IP network, such as:

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

Consult with your data network administrator. Refer also to the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103). Refer to "Related information products" on page xxiv for information on obtaining this document.

Once you understand this information, determine the QoS settings that you want, then configure them on each RLC port. For instructions, refer to "Configuring QoS" on page 211.

If IP mode is not the first stage in your network implementation, run this stage with a minimal number of users until you are sure that QoS on your IP network is acceptable. When you are satisfied with QoS transitioning performance, deploy the capability to the entire network.

If you are configuring QoS Transitioning Technology for Remote Office 911x series units, on the RLC you must configure at least one DSP device with the DSP load "911X". Each DSP device configured with the DSP load "911X" supports four modem channels.

Chapter 3

Installing the RLC

In this chapter

General safety

This section describes general safety guidelines recommended by Nortel Networks, and tools needed for installation. Follow the safety guidelines and recommendations in this chapter whenever you perform installation or maintenance tasks on the RLC.

CAUTION

Risk of data loss or equipment damage

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

Precautionary messages

This guide provides warnings related to hardware installation and handling, such as the preceding caution. For a description of these warnings, refer to “Conventions used in this guide” on page xxii.

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, as 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 installation tools

This section describes the tools necessary for RLC installation.

Required tools for hardware installation

You need the following tools for hardware installation:

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

Required tools for software installation or upgrade

You need the following items for software installation or upgrade:

- *Remote Office Product CD-ROM*
- PC with a CD-ROM drive or an Internet connection for obtaining software, firmware, and documentation updates
- 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

Before you unpack the equipment, ensure that your work area is safe from electrostatic discharge. For more details, refer to “Electrostatic discharge safety precautions” on page 78. Before you install the RLC, ensure that the package contents are all present and are not damaged.

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

Installing DSP application modules

Install DSP application modules (NTDR73xx) in the expansion slots on your RLC. This increases the number of simultaneous ports, and telephone lines, that you can use at remote sites. To add DSP application modules to your RLC, follow these procedures:

1. Determine the number of DSP application modules that meets your needs using the System expansion worksheet on page 343.
2. Install DSP application modules using the procedure on page 82.

Determining how many DSP application modules to add

To determine the number of DSP application modules your RLC needs, refer to the System expansion worksheet on page 343. For more information on how DSP application modules fit into your Remote Office system, refer to "DSP requirements" on page 49.

After receiving the DSP application modules from Nortel Networks, install them according to the procedure found under "Installing DSP application modules" on page 82.

Handling DSP application modules

Before beginning the installation and configuration process, review "General safety" on page 78. Follow the safety precautions and warnings found there to protect your investment in your telecommunications network.

CAUTION

Risk of data loss or equipment damage

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

Installing DSP application modules

To install DSP application modules:

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

   Note: Keep the DSP application modules in their antistatic bags.
3. Move the RLC from the host PBX to the work area.
4. Remove a DSP application module from its antistatic bag, holding it by its edges, with the insertion tabs facing down.
5. Insert the tabs into a pair of expansion slots on the RLC. (Refer to the illustration on page 6 for location of expansion slots.) The tabs snap into place when fully inserted. Visually inspect each tab to make sure that there is no gap and that the tab is fully inserted.

Identifying the cables

Cable your RLC according to the needs of your system. The following table identifies the cables available from Nortel Networks according to the connectivity provided by each.

IF you use the	THEN you can connect to
RLC Multi-I/O cable–Basic (NTDR79xx),	the PSTN. the Voice over Internet Protocol (VoIP) network.
RLC Multi-I/O cable–Enhanced (NTDR80xx),	the PSTN. the Voice over Internet Protocol (VoIP) network. locally connected telephones.

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

RLC Multi-I/O cable–Basic (NTDR79xx)

The RLC Multi-I/O cable–Basic provides three connections. Any number of RLCs in any card slot can use the Basic cable.

The following table outlines the connections provided by the RLC Multi-I/O cable–Basic.

The connector labeled	is a	that transmits	and connects to the
P1	25-pair connector (female)	all signals	I/O panel.
Note: For a 32-port RLC, insert **P1** into the socket for the first card slot occupied by the RLC.			
P2	DB-15 connector (male)	10BaseT signaling	CLAN Ethernet (customer LAN on the network).
Note: P2 requires a DB-15 to RJ-45 converter (shipped with the cable).			
P3	DB-9 connector (female)	RS-232 signaling	serial port to admin PC for administration and maintenance.

Refer to page 11 for an illustration of the RLC Multi-I/O cable–Basic.

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

The RLC Multi-I/O cable–Enhanced provides six connections. You can purchase the RLC Multi-I/O cable–Enhanced separately from Nortel Networks.

Note: Special rules apply if using more than one RLC Multi-I/O cable–Enhanced in one Meridian 1 PBX 11 cabinet. For further details, contact your Nortel Network distributor.

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

The connector labeled	is a	that transmits	and connects to the
P1	female 25-pair connector	all signals	I/O panel.
Note: If you are using a 32-port RLC, insert **P1** into the socket for the first of the two card slots occupied by the RLC.			
P2	male DB-15 connector	10BaseT signaling	CLAN Ethernet (customer LAN on the network).
Note: In North America, P2 requires a DB-15 to RJ-45 converter (shipped with the cable). Outside North America this plug is a female RJ-45 connector.			
P3	female DB-9 connector	RS-232 signaling	serial port to admin PC for administration and maintenance.
P4	male DB-15 connector	10BaseT signaling	ELAN Ethernet (host PBX's embedded LAN).
Note: In North America, P4 requires a DB-15 to RJ-45 converter (shipped with the cable). Outside North America this plug is a female RJ-45 connector.			
P5	male 25-pair connector	TCM signaling	cross-connect to local telephones.

Notes:

- Refer to page 13 for an illustration of the RLC Multi-I/O cable–Enhanced.
- The illustration on page 15 shows the RLC Multi-I/O cable–Enhanced used in installations outside North America.

Installing the Reach Line Card

The process of installing the Reach Line Card (RLC) involves:

- preparing the switch
- placing the RLC into its slot
- connecting the cables to the RLC

In systems with multiple RLCs, the process is the same for each one.

Preparing for installation

Configure the RLC's slot as if it were to hold an Extended Digital Line Card (XDLC). Refer to the documentation specific to your PBX for the exact procedures.

Split-slot wiring

If you use a NT8D37AA IPE cabinet, refer to the important note concerning the wiring of these cabinets on page 3.

Installing an RLC

To install an RLC:

1 Insert the RLC into its card slot.

Ensure that the tips of the ejector tabs are inside the front edges of the shelf when the card is fully inserted.

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

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

Refer to "LED indicators" on page 8 for the sequence of events that signify a successful RLC installation.

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

Note: When you run diagnostic tests after installing a double-slot RLC into a CS 2100 PBX, the second slot fails. Ignore the diagnostic test.

Connecting the cables to an RLC

To connect the cables for an RLC:

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

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

IF installing the	THEN proceed to
RLC Multi-I/O cable–Basic,	step 2.
RLC Multi-I/O cable–Enhanced in North America,	step 2.
RLC Multi-I/O cable–Enhanced in a location other than North America,	step 3.

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

Note: The RLC Multi-I/O cable–Enhanced ships with this adapter. This adapter is not an active transceiver.

a. Plug one end of a *shielded* (to meet CISPR B requirements) CAT 5 data cable of sufficient length to reach your Ethernet hub into the other side of the DB15 to RJ45 adapter connected to P2.

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

c. Proceed to step 4.

3 Plug **P2**, the male DB-45 connector into a female RJ-45 connector at one end of a *shielded* (to meet CISPR B requirements) CAT 5 data cable of sufficient length to reach your Ethernet hub.

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

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

IF installing the	THEN proceed to
RLC Multi-I/O cable–Basic,	"Verifying the installation" on page 89.
RLC Multi-I/O cable–Enhanced in North America,	step 5.
RLC Multi-I/O cable–Enhanced in a location other than North America,	step 6.

5 Plug **P4**, the second male DB-15 connector of the RLC Multi-I/O cable–Enhanced, into a DB15 to RJ45 adapter (NT7R93CA).

Note: The RLC Multi-I/O cable–Enhanced ships with this adapter. This adapter is not an active transceiver.

a. Plug one end of a *shielded* (to meet CISPR B requirements) CAT 5 data cable of sufficient length to reach your Ethernet hub into the other side of the DB15 to RJ45 adapter connected to P2.

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

c. Proceed to "Verifying the installation" on page 89.

6 Plug **P5**, the second 25-pair connector, into the cross-connect device serving the local telephones that you want to attach to RLC ports not needed for remote service purposes.

Verifying the installation

Once you have finished installing your RLC and connecting the cables, verify that you have completed these procedures properly according to the indications discussed below.

Indications of proper installation

An RLC automatically performs a self-test when inserted into its card slot. A successful self-test indicates proper installation. The Maintenance LED confirms a successful self-test by:

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

Note: Refer to “LED indicators” on page 8 for a further explanation of LED indicator behavior at startup.

Indications of proper cable connections

The ability to successfully log on to the RLC using Configuration Manager software indicates proper cable connections at the RLC. To perform this task, install the software first (refer to page 90). Once this task is completed, continue with “Starting Configuration Manager” on page 93.

Confirm the cable connections before attempting the troubleshooting procedures.

Note: If the RLC cables are properly connected and you still cannot log on, refer to Chapter 8, “Troubleshooting”.

Installing Configuration Manager software

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

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

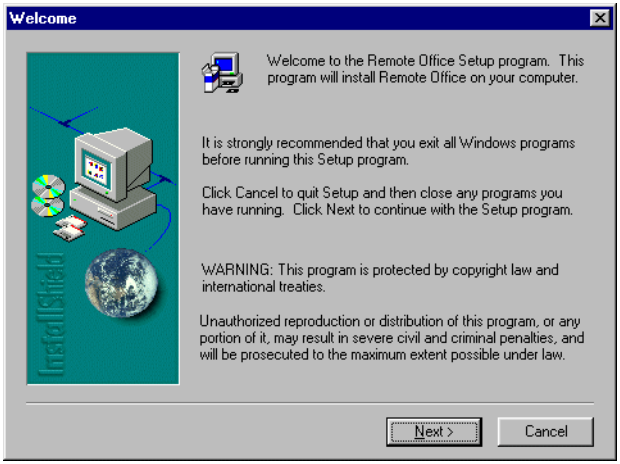
To install the software:

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

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

2 If autorun has started, select the Install option; otherwise, navigate to the software directory, and then locate and double-click on the setup.exe icon.

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

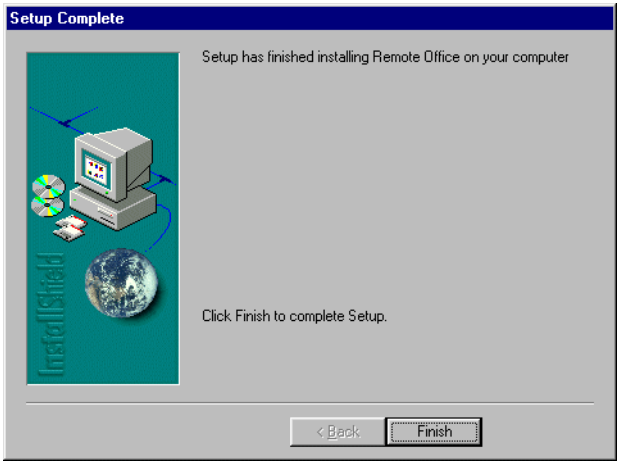


3 Click on the **Next** button, and then follow the screen prompts.

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

4 Click on the **OK** button.

Result: The Setup Complete screen displays.



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

5 Click on the **Finish** button.

Result: The InstallShield closes.

Using the Configuration Wizard to perform initial configuration

The Configuration Wizard option in Configuration Manager allows you to configure the minimum information needed for establishing communications between the RLC at the host site and the following remote-site products:

- Remote Office 9110
- Remote Office 9115
- Remote Office 9150
- Meridian Digital Telephone Internal IP Adapter
- Meridian Digital Telephone External IP Adapter

The Configuration Wizard provides only a subset of the full configuration settings available in Configuration Manager. However, by using the Configuration Wizard, the RLC 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 RLC (online mode).

What you can configure with the Configuration Wizard

The Configuration Wizard allows you to configure the following elements:

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

  This information must be valid for your IP network.

  Note: If you do not plan to use 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, the procedure on page 98 provides sample information.
- for Voice over IP capability:

  — the IP addresses for each remote unit connected to the RLC
- for PSTN capability:

  — the RLC port used for connection to the remote unit

  — the telephone number of the remote unit

Ensure that 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.

Starting Configuration Manager

To start Configuration Manager:

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

Result: Configuration Manager opens and displays the Local User Authentication dialog box, similar to the following, prompting you for the login name and password:

2 Enter **admin** in the Login Name field.

3 Enter **root** in the Password field.

4 Click on the **OK** button.

Result: The Configuration Manager dialog box displays informing you of a successful log on.

5 Click on the **OK** button.

Result: The Configuration Manager dialog box closes.

6 Do one of the following:

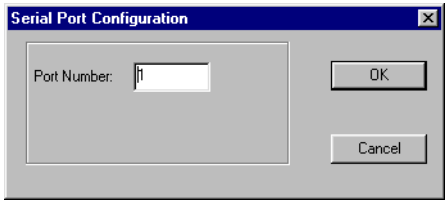
IF you want to perform an	THEN
offline configuration,	■ Choose View → Device Type → RLC. ■ Continue with "Performing configuration with the Configuration Wizard" on page 97.
online configuration,	continue with "Establishing a serial connection" on this page.

Establishing a serial connection

To establish a serial connection:

1 From the Menu Bar, choose Connect → Logon Unit → Serial.

Result: The Serial Port Configuration dialog box displays, similar to the following:



2 Enter the COM port number the unit is connected to in the Port Number field, and then click on the **OK** button.

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

3 Enter **guest** in the Login Name field.

4 Enter the default password, **guest123**, in the Password field.

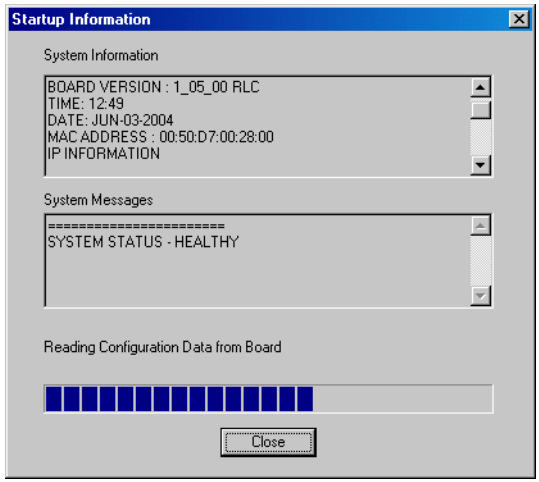
Note: Nortel Networks recommends that you do not change the password until your system is up and running.

5 Click on the **OK** button.

Result: Configuration Manager initiates a connection attempt and displays the following message:

```
Trying Connection
```

IF the logon attempt	THEN
fails,	the following message displays: `10060 SERIAL CONNECTION FAILED` Check the serial connection and ensure it is good. Then, go back to step 1.

IF the logon attempt	THEN
is successful,	the User Logged In dialog box displays. Click on the **OK** button. **Result:** The Startup Information dialog box displays, similar to following:  Messages similar to the following display above the progress bar at the bottom of the dialog box: ■ Reading Hardware Information ■ Reading DSP Load Data ■ Reading Configuration Data These messages indicate that Configuration Manager is obtaining the unit's configuration information from Flash memory. Click on the **Close** button.

Performing configuration with the Configuration Wizard

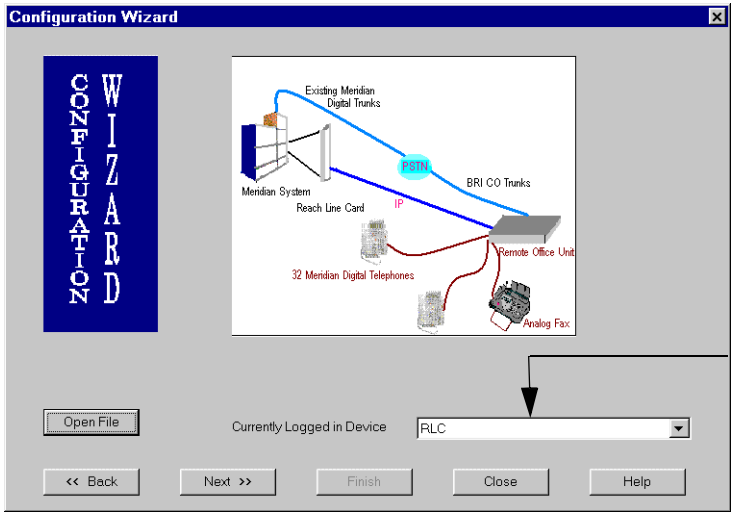
To perform configuration with the Configuration Wizard:

1 From the Menu Bar, choose Configuration Wizard.

Result: The Configuration Wizard screen displays, similar to the following:

2 After reviewing the message, click on the **Next** button.

Result: The Configuration Wizard screen displays, similar to the following:



Ensure the Device field shows RLC.

3 Verify that the Currently Logged in Device drop down box shows RLC. If it does not show RLC, select RLC from the drop down list.

4 Click on the **Next** button.

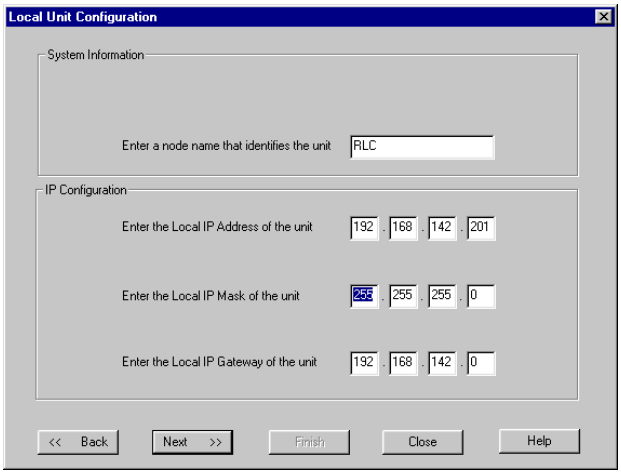
Result: The Local Unit Configuration dialog box displays. A completed example is shown on page 99.

5 Complete the fields in this dialog box as described in the following table:

Field	Description
Enter a node name that identifies the unit	Enter a name to describe the RLC you are configuring.
Enter the local IP Address of the unit	Enter the IP address assigned to the RLC. **Note:** The system requires that you enter an IP address. If you are using PSTN only, enter the following: **1.2.3.4**.

Field	Description
Enter the Local IP Mask of the unit	Enter the subnet mask. **Note:** The system requires that you enter an IP address. If you are using PSTN only, enter the following: **255.255.0.0**.
Enter the Local IP Gateway of the unit	Enter the IP address of the gateway between the RLC and the network. **Note:** The system requires that you enter an IP address. If you are using the PSTN only, enter **1.2.3.5.** as both the IP address on the administration PC and gateway on the RLC.

The following is a completed example:



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

6 Click on the **Next** button.

Result: The Set the Remote Unit information dialog box displays. A completed example is shown on page 102.

7 Complete the fields on this dialog box as described in the following table:

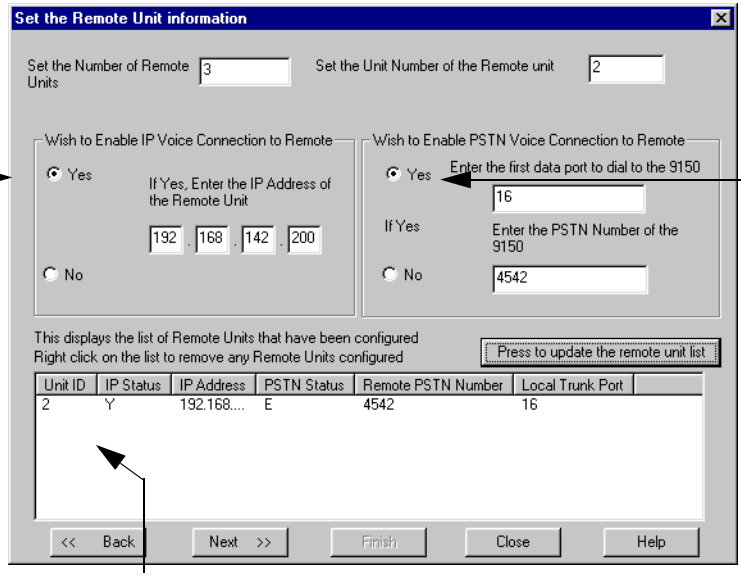
Field	Description
Set the Number of Remote Units	Enter the number of remote units you plan to connect to this RLC.
Set the Unit Number of the Remote unit	Enter the number that uniquely identifies the remote unit record you are configuring. **Note:** You must give each unit that is connected to the same RLC a unique unit record number. Do not confuse this number with the unit ID (described below).
Set the Unit ID of the Remote Unit	Enter the number between 1 and 255 that differentiates the unit being configured from every other RLC or remote unit in your remote network. This number must be different from: ■ the number assigned to the RLC that this remote unit connects to ■ the numbers assigned to other remote units connected to the same RLC
Wish to Enable IP Voice Connection to Remote	■ Click on the **Yes** option button to enable voice over IP connection to the Remote Office unit. Then enter the Remote Office unit's 32-bit, decimal dot notation address (xxx.xxx.xxx.xxx). This is not the URL (www.) site name. ■ Click on the **No** option button to disable voice over IP connection to the Remote Office unit. Clicking on the No option button dims the IP Address fields.

Field	Description
Wish to Enable PSTN Voice Connection to Remote	■ Click on the **Yes** option button to enable PSTN connection to the Remote Office unit.Then complete the following steps: **a** Enter the number of the RLC port that you want to dedicate for connections to this remote unit. **Note:** The port must be a PBX data port. **b** Enter the telephone number that must be dialed to connect to the remote unit. The telephone number can include the following digits or characters: 0 through 9, #, *, comma (,), period (.), and dash (-). ■ Trunk access digit delimiter: "#" (pound/number sign) ■ Caller ID separator and 1/2 second delay: "," (comma) ■ Caller ID separator: "." (period) ■ null separator: "-" (dash) Refer to "Configuring 10-digit ISDN numbers" on page 202 for more information. ■ Click on the **No** option button to disable the PSTN connection to the Remote Office unit. Clicking on the No option button dims the PSTN Number fields.

8 Click on the **Press to update the remote unit list** button.

Result: The information entered for this remote unit displays in the list of configured remote units in the lower half of the Set the Remote Unit information dialog box.

The following is a completed example:



Click on the **Yes** option button to allow voice calls over IP, then enter the remote unit's IP address.

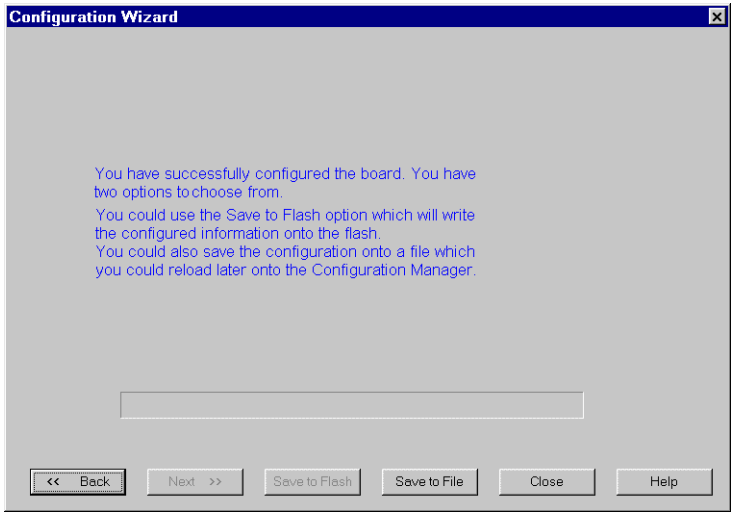
Click on the **Yes** option button to allow voice calls over the PSTN, then enter the remote unit's phone number.

This table allows you to configure connections for more than one remote unit.

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

10 Click on the **Next** button.

Result: The following screen displays:



11 Do one of the following:

IF you are performing an	THEN
offline configuration,	■ Click on the **Save to File** button. ■ **Result:** Configuration Manager prompts you to specify the directory path and file name for the configuration file. ■ Specify the directory path and file name for this configuration. ■ **Note:** The file name automatically defaults to the name you entered as the node name. ■ Ensure the Files of type field shows Text File (*.TXT). ■ Click on the **Save** button to complete the Save to File. ■ **Result:** The file is saved, then you are asked if you want to configure another board. If you do, click on the **Yes** button and continue with step 3 on page 98. ■ You can open the information in this file in Configuration Manager, then send and save the file in the RLC's Flash memory at another time. For instructions, refer to "Working with configuration files" on page 145.

IF you are performing an	THEN
online configuration,	■ Click on the **Save to Flash** button. ■ **Result:** Configuration Manager writes the information entered to the Flash memory of the RLC you are configuring. ■ If successful, Configuration Manager displays the following message: `Data Sent Successfully` ■ **Note:** Nortel Networks recommends that you also save the configuration to a file. For instructions on how to do this with Configuration Manager, refer to the documentation for your unit. ■ Restart the RLC.

Testing the network connections

Use the following methods to test the connections to the RLC:

- Check your system's host-site connections to ensure basic PSTN and IP network connectivity.
- Perform a PING test. To perform this test, the following must be true:
  — The RLC must be physically connected to the IP network.
  — A link LED indicator must be on.
  — You must be physically connected to the network.
  — You must be logged on to Configuration Manager.
  Refer to "Using Configuration Manager PING" on page 312 for complete details on performing a Configuration Manager PING.
- Perform a PSTN connectivity test.
  Refer to "PSTN connectivity testing" on page 315 for complete details on performing a PSTN connectivity test.
- Perform a syslog test.
  Refer to "Syslog testing" on page 320 for complete details on performing a syslog test.

Check host site connections

When testing the connections in your remote services network, you must first confirm that the equipment is connected properly at the host site.

Telephone network connections

Check the following points in your telephone network connection:

- Confirm that the proper connections are made for the digital telephones at the cross-connect system in your corporate switch room.
- Confirm that the RJ11 plug of the telephone wire leading to the digital telephone is properly and securely seated in the RJ11 jack in the wall.
- Confirm that the RJ11 plug at the other end of the telephone wire is properly and securely seated in the RJ11 jack at the base of the digital telephone.

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

- Confirm that the 25-pair connector of Plug 5 and the 25-pair connector of a cable leading to your cross-connect are properly and securely joined.
- Confirm that the 25-pair connector at the other end of the cable mentioned in the previous step is properly and securely joined to the 25-pair socket of the cross-connect.
- Confirm that the cable leading from the RLC to the cross-connect is in good condition, end-to-end.

Ethernet connection

Check the following points in your Ethernet connection:

- Confirm that the DB15–RJ45 adapter at Plug 2 of the RLC Multi-I/O cable–Enhanced is properly and securely joined to Plug 2.
- Confirm that the RJ45 plug of a CAT5 data cable leading to your Ethernet hub is properly and securely seated in the RJ45 socket of the DB15–RJ45 adapter mentioned in the previous step.
- Confirm that the other end of the CAT5 data cable mentioned in the previous step is properly and securely seated in the appropriate Ethernet hub socket.
- Confirm that the CAT5 data cable leading to your Ethernet network's data router is properly and securely seated in the appropriate Ethernet hub socket.
- Confirm that the CAT5 data cable leading from your Ethernet hub is properly and securely seated in the appropriate socket of the data router mentioned in the previous step.

Chapter 4

Configuring the host PBX for the RLC

In this chapter

Configuring the host trunk for a Remote Office 9150 unit

Remote Office 9150 units require an end-to-end digital connection. Tell your service provider which type of ISDN connection (PRI or BRI) that you need for your remote service equipment. Nortel Networks recommends ISDN PRI trunks for connecting the CO to the host PBX. Tell your service provider the parameters to configure on the trunk according to the features that you want on the devices at your remote location.

ISDN PRI configuration

ISDN PRI trunks transport Remote Office 9150 unit calls between the host PBX and the PSTN. To ensure full functionality for all remote sites served by each RLC, ask your service provider to configure the following elements on each trunk:

- two-way voice and two-way data capability
- caller ID
- end-to-end digital circuitry, no analog segments (confirm this with both long-distance and local service providers)
- non-blocking configuration (ensure that configuration will not block remote site traffic)
- 56K or 64K clear channel, according to your equipment

ISDN BRI configuration

Some locations require ISDN BRI service from the host PBX (the host trunk connection) instead of PRI for geographical reasons. ISDN BRI configuration is identical to ISDN PRI configuration. Verify this with your service provider. For information about ordering BRI service, refer to the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103). For information on how to obtain this document, refer to “Related information products” on page xxiv.

Note: In North America, an ISDN BRI line can only be ordered as a subscriber line and is not a valid trunk option.

Configuring an RLC slot

For the host PBX to communicate properly with RLCs, you must configure each RLC slot as an Extended Digital Line Card (XDLC) slot. Refer to the documentation for your PBX to complete this procedure.

Understanding port relationships

This section focuses on the relationship between the two principle RLC ports in a system using the PSTN:

- remote ports
- network ports

ATTENTION This section is critical to your understanding the operation of the Reach Line Card.

Functionality provided by the various port types

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

- a remote port

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

- a network port

  Network ports place and receive PSTN calls to and from remote devices. Network ports require only the most basic configuration on the host PBX that allows this port to place and receive calls of the appropriate type for the particular remote unit. RLC network ports do not use PBX features such as conference or call forward.

  When QoS on the IP network degrades, QoS Transitioning Technology opens PSTN connections using paths provided by the network ports. Refer to “Configuring QoS” on page 211 for information on configuring QoS thresholds.

- a local TCM port

  Local TCM ports support local telephones connected at the host PBX.

Configuring remote and network ports

Observe the following rules when configuring remote and network ports for Remote Office systems.

General

Basic Remote Office configuration starts with the guidelines listed in this section.

- Configure one remote port for each remote device, such as a digital telephone or a fax machine, that you want the RLC to support.
- Configure at least one network port for each Remote Office unit that you want to support with the RLC.

Note: Each network port provides up to 64K of PSTN bandwidth between the RLC and the Remote Office 9150 unit. To provide 256K of bandwidth between the RLC and a Remote Office 9150 unit, configure four network ports. For the specific procedure to configure remote and network ports, refer to the documentation for your PBX.

At your PBX administration terminal, configure voice ports to the appropriate RLC remote ports supporting remote digital sets using any of the following:

- Remote Office 9150 units
- Remote Office 911x units
- Meridian Digital Telephone Internal IP Adapters
- Meridian Digital Telephone External IP Adapter
- Analog Telephone Adapters (ATAs)

Note: Remote Office 911x units do not support ATAs.

RLCs

One 16-port RLC supports a maximum of eight Remote Office 9150 units, 16 Remote Office 911x series units, or 16 Meridian Digital Telephone IP Adapter units.

One 32-port RLC supports a maximum of four Remote Office 9150 units, 20 Remote Office 911x series units, or 20 Meridian Digital Telephone IP Adapter units.

Remote Office 9150 units

Every port on a single Remote Office 9150 unit must be served by the same RLC.

Digital telephone sets connected to Remote Office 9150 units do not support DRG2, DRG3, or DRG4. These same digital telephone sets support DRG1, the default ring.

Remote Office 911x series units and Meridian Digital Telephone IP Adapter units

Associate every Remote Office 911x unit or Meridian Digital Telephone IP Adapter unit with one port on an RLC.

Refer to your PBX documentation for the exact procedures and a complete list of possible settings for voice and data ports.

Digital telephone sets connected to Remote Office 911x series units and Meridian Digital Telephone IP Adapter units do not support DRG2, DRG3, or DRG4. These same digital telephone sets support DRG1, the default ring.

Remote port configuration

Configure each remote port on the host PBX according to the device connected to it at the remote site. If that device is a telephone, configure the port with all the features (for example, voice mail and call transfer) that you want.

- On the host PBX, configure ports for all remote service digital telephones as voice ports.
- On the host PBX, configure ports for all remote service MCA data adapters supported by the RLC as data ports (Remote Office 9150 units only).

- If you have enough data ports available on your Remote Office 9150 unit, configure ATA data adapters supported by the RLC as data ports on the host PBX. If you do not have enough data ports available, you can set up ATAs on voice ports on the host PBX.

Note: Remote Office 911x series units do not support data adapters.

Fax relay support

You can use the following compression algorithms for fax transmission:

- G.711

  If you select G.711, then faxes are transmitted at 64 Kbps. In this mode, the fax protocol is not interpreted. Therefore, all non-standard fax features are supported regardless of the manufacturer.

- G.729A/Fax

  If you select G.729A/Fax, then the fax protocol is interpreted, and the fax modem is demodulated in an attempt to reduce the amount of bandwidth that is consumed. In this mode, the fax transmission is restricted automatically to 9.6 Kbps. The G.729A/Fax algorithm provides more bandwidth efficiency at the expense of greater protocol-sensitivity and potentially lower fax speeds.

Note: Error Correction Mode (ECM) is automatically disabled during fax relay.

Configuration for fax relay support

On the host PBX, you must configure the TN associated with any remote analog ports (ATA or the Remote Office 9150 unit analog port) as a voice port.

Do this by ensuring that the remote ATA devices, or the Remote Office analog port, map to an ATA port on the RLC. ATA ports were introduced in release 22 of Meridian system software. The ATA is in the data port range, but the class of service treats the TN as a voice TN.

You can map remote analog ports (that are in the voice port range on any supported release of Meridian software) to non-ATA voice ports on the RLC.

PBX

Configure the host PBX as follows:

1. Program the data TN for a digital set.
   a. If you have a telephone programmed against the voice TN, then the data TN telephone type must be the same as the voice TN telephone type. For example, if the telephone on voice TN 6 15 is a 2616 then the fax data TN 6 31 must be programmed as 2616.
   b. Set DTAO = MCA
   c. Set the DN of the fax machine or ATA on Key 0 of the data TN.
2. After programming the data TN, go back in again to change the CLS. Do one of the following:
   - If the system software includes package 186, program an ATA by adding CLS=FLXA VCE CPTD.
   - If you do not have package 186 then, add CLS =FLXA VCE.
3. Enable the TN in LD 32.

RLC

Configure the corresponding ports on the RLC as follows:

1. Access Configuration Manager → RLC → RLC Port Configuration.
2. On the RLC port that matches the ATA port, configure the compression, priority and usage. This port must also be configured as a remote port, not a network port.
3. Click on the **OK** button on the RLC Port Configuration window, send to unit, save configuration to Flash and reboot the unit.

   Notes:

   a. When you save configuration changes to Flash, the system suspends new call processing for approximately 30 seconds.
   b. If you intend to use a fax on the ATA device, or you are programming the 9150 fax port, Nortel Networks recommends using the G.729A/Fax compression algorithm.

Remote Office 9150 unit

Configure the Remote Office 9150 unit as follows:

1 For the Remote Office 9150 fax port, do the following:

   a. Access Configuration Manager → 9150 → 9150 Port Configuration.

   b. Map port 64 on the Remote Office 9150 unit to the data port on the RLC.

   c. For an ATA adapter, map the 9150 port that is 16 ports above the telephone that house the ATA adapter. For example, if the telephone housing the ATA is on the Remote Office 9150 unit and is wired to port 0, then the ATA is configured on the Remote Office 9150 unit port 16.

   d. Map the ATA port to the RLC data port configured on the host PBX.

2 Verify that any other unused Remote Office 9150 port that has the same RLC port number as the Fax or ATA is configured as Local.

   For example, if the RLC data port 31 (mapped to 9150 port 64) is being used for fax, make sure the Remote Office 9150 unit port 31 is set to local only. This prevents any possibility of port contention occurring at the host side.

   Also, make sure that the telephone type for the ATA port is selected as ATA not as a digital set.

3 For LOCAL 9150 access only from the Remote Office 9150 unit, configure the ATA port Local Call Key1 to Key Number 0.

4 If the port is configured for local and remote, verify that Forward Busy/No Answer is disabled.

5 Click on the **OK** button on the 9150 Port Configuration window, then click on the **Send** button.

6 From the Upload/Download menu option, select Save to Flash.

   Note: When you save configuration changes to Flash, the system suspends new call processing for approximately 30 seconds.

7 Reboot the unit.

Network port configuration

Configure the RLC network ports that are connected to Remote Office 9150 units as MCA data adapters with the first line able to place and receive data calls. Configure the 911x network ports on the RLC as voice ports with flexible voice/data allowed. To configure data ports, refer to “Sample configuration files” on page 349.

- If the RLC and its remote units connect only through the IP network, you do not need to configure network ports for the RLC. The RLC and remote units use an IP path to communicate with one another.
- If your system uses both the IP and PSTN connections to route calls, configure a sufficient number of network ports for the RLC to handle the anticipated traffic between the remote units and the host PBX.
- Remote Office 911x series units do not support MCAs.
- Remote Office 911x series units do not support ATAs.

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

Meridian 1 PBX network port configuration for a Remote Office 9150 unit

To support a Remote Office 9150 unit on a Meridian 1 PBX, you must configure the RLC network port as follows:

- Class of Service: DTA, FLXD
- DTAO prompt must be configured as MCA
- BRI CLS must include: VCE DTA
- TSP must set to USID = 0 to provide the BRI connection from the Meridian 1 PBX.

Note: For the CS 2100 PBX, similar configuration rules apply. For configuration requirements, refer to “CS 2100 configuration requirements” on page 119.

Meridian 1 PBX network port configuration for a Remote Office 911x series unit

To support a Remote Office 911x series unit on a Meridian 1 PBX, you must configure the RLC network port using the same procedure as described for PBX configuration for ATA. Refer to “PBX” on page 114 for details.

Note: For the CS 2100 PBX, similar configuration rules apply. For configuration requirements, refer to “CS 2100 configuration requirements” on page 119.

RLC and Remote Office 9150 unit connection paths

The RLC network ports (used to connect to the Remote Office 9150 units) carry HDLC-framed data. You must configure these ports so that they can transparently pass this data.

Any port you configure as a data port on the Meridian 1 PBX can be an RLC network port.

If the Meridian 1 PBX, instead of the PSTN or a PTT, provides the Remote Office 9150 unit’s ISDN number, you must configure the line on the host PBX (LD 27 on the Meridian 1 PBX) as follows:

1 Set B1CT to VCE and DTA.

2 Set B2CT to VCE and DTA.

3 Set USID to 0.

PBX trunks and RLC network ports

When using the Remote Office unit with PSTN connectivity, the PBX trunks must provide data capability. To make sure that the PBX is ready for data calls, complete the following outlined checkpoints:

1 Use the PRT command in LD20 on the PBX to print out the Network Port TNs that have been provisioned against the RLC slot. Make note of the TGAR and NCOS values.

Note: For specific printing instructions, refer to your PBX documentation.

2 Print out the PBX Route Data Block (RDB) in LD 21. For each PRI:

a. Review the TARG values. If the values match the Network Port TGAR, calls are NOT allowed through the PRI.

b. Review the trunk capability at the DSEL prompt. It must be “Voice or Data” (VOD) or “Data Only” (DTA).

c. Check that the ICOG prompt is Incoming and Outgoing (IAO).

Note: If you make changes to the DSEL, or the ICOG prompt, make sure that the central office is configured likewise, that is to say, changing the DSEL from VCE to VOD can be ineffective because the CO still rejects data calls.

3 Print out the PBX trunk time slot configuration information in LD 22 CEQU. Ensure that there is an adequate number of time slots provisioned with data capability. Here is an example of the printout:

```
(data omitted)

DLOP NUM DCH FRM LCMT YALM TRSH
TRK  001  24  D4  AMI  DG2  00 <-- DTI trunks
     012  24  D4  AMI  DG2  00
PRI  003  24 ESF  B8S  FDL  00 <-- PRI trunks - voice or data
     051  00 ESF  B8S  FDL  00
```

A DCH setting of 0 indicates that 0 time slots are usable for data call capability. The default setting is 24.

Note: The above example displays the North American default values.

4 If the RLC is dialing to the Remote Office unit, and the number being dialed is using the PBX routing (for example. 9 or 6 access code), you need to make sure that the call is presented to the PRI trunk and not a standard CO trunk.

Verify that the Network Port TN NCOS has the capability to access the PRI. One way to ensure that the PRI is accessed is to use the Trunk Access code (ACOD) which was printed in step 2.

You can modify the RLC Remote Connection PSTN information to use the ACOD to directly access the trunk. For example, set the Remote Connection number to be #8002#5551212, assuming that 8002 is the trunk ACOD and you are placing a local call.

How the remote and network ports work together

RLCs configured as PSTN-only, or in QoS transition situations, route voice traffic through the PSTN. a call placed to voice port 0 can be relayed to a Remote Office 9150 unit configured as PSTN-only. For this call, the RLC calls the Remote Office 9150 unit using the dedicated network port for that unit. Each network port on a Remote Office 9150 unit supports up to eight simultaneous calls using G.729A (8 Kbps) compression. For Remote Office 911x units, each network port supports only one call, regardless of compression.

CS 2100 configuration requirements

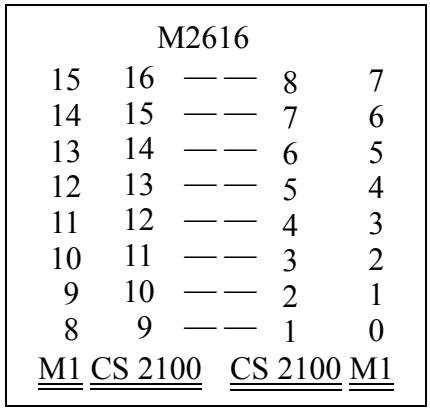
This section describes the CS 2100 PBX configuration that is needed to support the Remote Office 9150 unit.

Note: You must configure the Remote Office 9150 unit operating behind a CS 2100 PBX using Meridian 1 PBX key numbering.

M2000 telephone set key numbering

The key numbering convention for M2000 series telephones on the Remote Office 9150 unit is different from the key numbering convention on the CS 2100 PBX.

On the Remote Office 9150 unit, keys are numbered from 0 through 15, whereas on the CS 2100 PBX, keys are numbered from 1 through 16. Refer to the following figure for a comparison:



M1 = Meridian 1 PBX
CS 2100 = Communication Server 2100

M0200 option on telephone set

M0200 must be assigned to the M2616 telephone set configuration on the CS 2100 PBX. Without this option, the M2616 telephone set does not function properly.

Port configuration

The port numbering on the RLC is different from the port numbering on the CS 2100 PBX. Refer to "RLC and CS 2100 port numbering comparison" below.

RLC and CS 2100 port numbering comparison

Port type	RLC port numbering	CS 2100 port numbering
Voice ports	0–15 and 32–47	Even-numbered ports
Data ports	16–31 and 48–63	Odd-numbered ports

RLC and CS 2100 port mapping

The following table identifies the port mapping between the RLC and the CS 2100:

16-port RLC				32-port RLC			
RLC voice ports	**IPE voice ports**	**RLC data ports**	**IPE data ports**	**RLC voice ports**	**IPE voice ports**	**RLC data ports**	**IPE data ports**
0	0	16	1	32	0	48	1
1	2	17	3	33	2	49	3
2	4	18	5	34	4	50	5
3	6	19	7	35	6	51	7
4	8	20	9	36	8	52	9
5	10	21	11	37	10	53	11
6	12	22	13	38	12	54	13
7	14	23	15	39	14	55	15
8	16	24	17	40	16	56	17
9	18	25	19	41	18	57	19
10	20	26	21	42	20	58	21
11	22	27	23	43	22	59	23
12	24	28	25	44	24	60	25
13	26	29	27	45	26	61	27
14	28	30	29	46	28	62	29
15	30	31	31	47	30	63	31

Sample datafill for network ports

For ISDN BRI connectivity and QoS transitioning functionality, each 64 Kbps trunk requires a dedicated data port on the RLC. On the CS 2100, you must configure this data port as a Meridian Communications Adapter (MCA) and datafill it as a 64K synchronous adapter. The following is an example of the SERVORD command used to provision a synchronous MCA adapter:

```
NEW $ 2386152 MCA MTL1 0 12 214 Y MCA N S 64000 I N N N N N 0
HAYES $ HOST 20 2 01 03 $

>QLEN  2386152
LEN:     HOST  20 2 01 03
TYPE: SINGLE PARTY LINE
SNPA: 214
DIRECTORY NUMBER:     2386152
LINE CLASS CODE:  MCA
CUSTGRP:            MTL1  SUBGRP: 0  NCOS: 12  RING: Y
DATA UNIT PROFILE:
CLASSDU: MCA       IDLETO: 0  DOWNLOAD: N
CONFIG:  DTE                  DTEIF: RS232C
SYNCHRO: S   DATARATE: 64000  CLOCKSRC: I
DUPLEX:  F                    KBDTYP: HAYES
HOTLINE: N   VLL: N   V.25: N   HDLC: N   RTS: N
DPOPTS:
CARDCODE:  DR68AA GND: N  PADGRP: NPDGP  BNV: NL MNO: Y
PM NODE NUMBER     :    105
PM TERMINAL NUMBER :    36
OPTIONS: NDC

KEY     FEATURE
NONE
```

M39xx Release 2 telephones with MCAs

When configuring RLCs for QoS Transitioning Technology, you must configure a data port as a Meridian Communications Adapter (MCA).

A patch is required for CS 2100 sites using only M39xx Release 2 telephones and PBX software versions MSL14 or earlier to allow QoS transition. This is due to the fact that CS 2100 PBXs using software version MSL14 or earlier and configured for only M39xx Release 2 telephones do not recognize MCAs.

The patch numbers are:

- JDT01.xxx
- JDT04.xxx

where xxx denotes the PBX version number.

Contact your Nortel Networks distributor to receive the patch.

Chapter 5

Using Configuration Manager

In this chapter

What is Configuration Manager?

Configuration Manager is a Windows-based software application that you install on your PC. Configuration Manager allows you to configure, administer, and upgrade the Remote Office 9150 unit. These tasks can be performed over either of the following connection types:

- 10BaseT Ethernet
- RS-232 serial

  Note: It is not possible to use Configuration Manager to configure an RLC or Remote Office unit over a modem connection.

The CD shipped in the Remote Office 9150 unit package includes the Configuration Manager software. You can obtain the CD from your Nortel Networks distributor or click on the **Support** link at the following website:

www.nortelnetworks.com

For the required characteristics of the Meridian administration PC, refer to "Windows PC requirements" on page 69.

To install the Configuration Manager software on your administration PC, refer to "Installing Configuration Manager software" on page 90.

ATTENTION

Complete all Remote Office configuration using Configuration Manager[i]. Only use the man-machine interface (MMI) with the assistance of technical support personnel for troubleshooting and diagnostic testing. For further details, refer to "Command line interface" on page 46.

i. Complete initial configuration of Remote Office 911x series and Meridian Digital Telephone IP Adapter units with the telephone set menu. Complete subsequent configuration updates of these units with Configuration Manager. For further information, refer to the *Remote Office 911x Installation and Administration Guide* (NTP 555-8421-220) or the *Meridian Digital Telephone IP Adapter Installation and Administration Guide* (NTP 555-8421-211).

Starting and viewing Configuration Manager

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. If you use larger fonts, some fields and buttons might be hidden. You must use the horizontal and vertical scroll bars to view the hidden fields or buttons. For instructions on changing your display settings, refer to the Windows online help on your PC.

To start and log on to a Configuration Manager session:

1 From the Menu Bar, choose Start → Programs → Remote Office → Configuration Manager.

Result: Configuration Manager opens and prompts you for the logon name and password.

2 Enter **admin** in the Login Name field.

3 Enter **root** in the Password field.

Note: This is the default password. You can change the password after installation, though Nortel Networks recommends that you do not change the password until your Remote Office system is up and running.

4 Click on the **OK** button.

Result: The system informs you of a successful logon. In the event of an unsuccessful logon, the system informs you of the need to re-enter the information.

5 Click on the **OK** button.

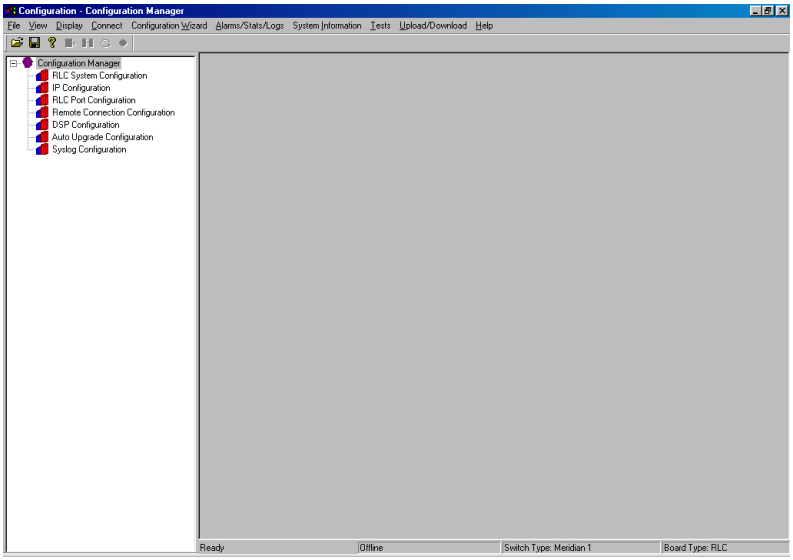
Result: The Local User Authentication dialog box closes.

6 Proceed as follows:

To perform an	Refer to
online configuration,	“Logging on to a unit” on page 149.
offline configuration,	“Selecting the device type for offline configuration” on page 148.

7 To view the system tree, click on 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. The following is an example:



Configuration Manager description

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.

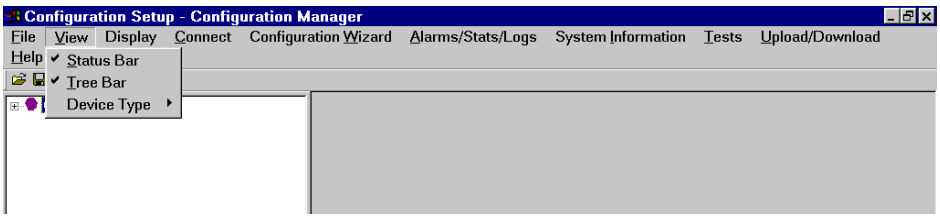
- The menu across the top of the screen lists various administrative tasks you can perform. These tasks are common to all Remote Office units.
- The pane on the left lists the property sheets you can work with. In this guide, the left pane is called the *system tree*.
- The pane on the right displays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

Menu Bar

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

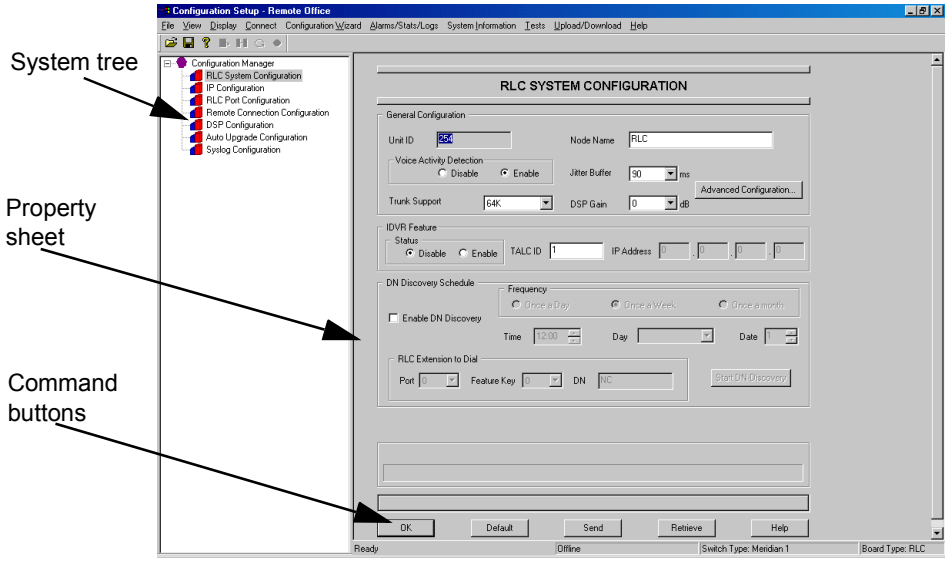
When you click on an option on the Menu Bar, a drop down list displays. When you select an option from the drop down list, the screen associated with that option displays.

Note: Options that are 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).



System tree

The left pane of Configuration Manager lists the property sheets you can access. To expand the list of all the property sheets associated with the logged-on or selected device, click on the plus (+) sign. (To hide the list, click on the minus [-] sign.) With the System Tree expanded, click on a configuration to display the associated property sheet in the right pane, similar to the following:



To hide the system tree, choose View → Tree Bar from the Menu Bar. The screen redraws itself showing only the right pane and displaying the selected property sheet. To display the system tree again, choose View → Tree Bar.

Property sheets

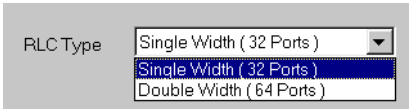
When you are logged on to a particular Remote Office unit (that is, a Remote Office 911x series unit, a Meridian Digital Telephone IP Adapter unit, a Remote Office 9150 unit, or an RLC), Configuration Manager displays a system tree specific to the logged-on unit.

Note: When working with a Meridian Digital Telephone IP Adapter unit in Configuration Manager, use Remote Office 911x property sheets.

When you click an item in the system tree, the associated property sheet displays in the right pane. For instructions on selecting a device type when not logged on, refer to "Selecting the device type for offline configuration" on page 148.

Drop down boxes

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



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

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

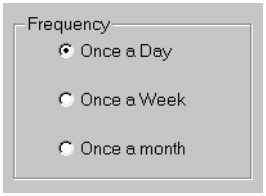
Check boxes

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 on the check box. A check mark displays. When you click on the check box again, the check box clears (thereby disabling the feature).

Option buttons

Some fields have multiple options. There is a circle beside each option that is called an *option button*. For these fields, you can only select one option.

To enable an option, click on its associated option button. If you change a previously selected option, the previously selected option button clears.



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

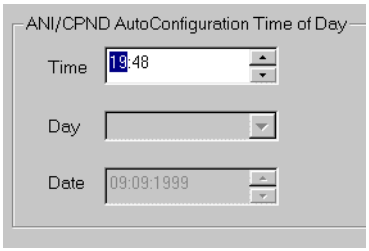
- Some fields are dimmed (disabled) because they cannot be configured in the context of the option you selected.
- Other fields are re-enabled (no longer dimmed).
- One or more values on the property sheet are replaced with values that are specific to the option you selected.

Scroll boxes

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

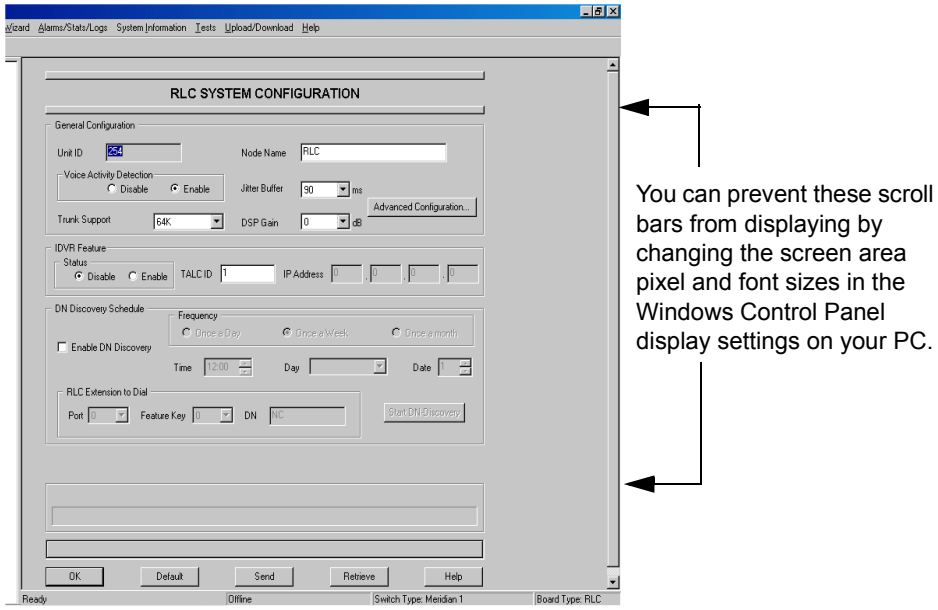


Scroll bars

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 display 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.



Command buttons

The following buttons display on every property sheet listed in the first level of the Remote Office Configuration Manager system tree (left pane):

- OK

  Click on this button to accept any changes you have made to the displayed property sheet. This command stores these values in a temporary file on your PC until you are ready to update the unit's Flash memory. For more details, refer to "OK" on page 140.

- Default

  Click on this button to insert default values into every field in the displayed property sheet.

- Send

  Click on this button to update the buffer of the unit you are logged on to with the values currently on the displayed property sheet. For more details, refer to "Send" on page 141.

- Retrieve

  Click on this button to display the saved configuration value for every field on the displayed property sheet from the unit's local buffer. The unit's local buffer contains the last sent data. For more details, refer to "Retrieve" on page 142.

- Help

  Click on this button to display online Help for the property sheet you are working with. For other methods of displaying Help, refer to "Using online Help" on page 136.

Using online Help

While using 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 on the **Help** button to get information concerning the active property sheet.
- Method 2: From the Menu Bar, choose Help → Help Topics.
- Method 3: Click on the **?** 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:

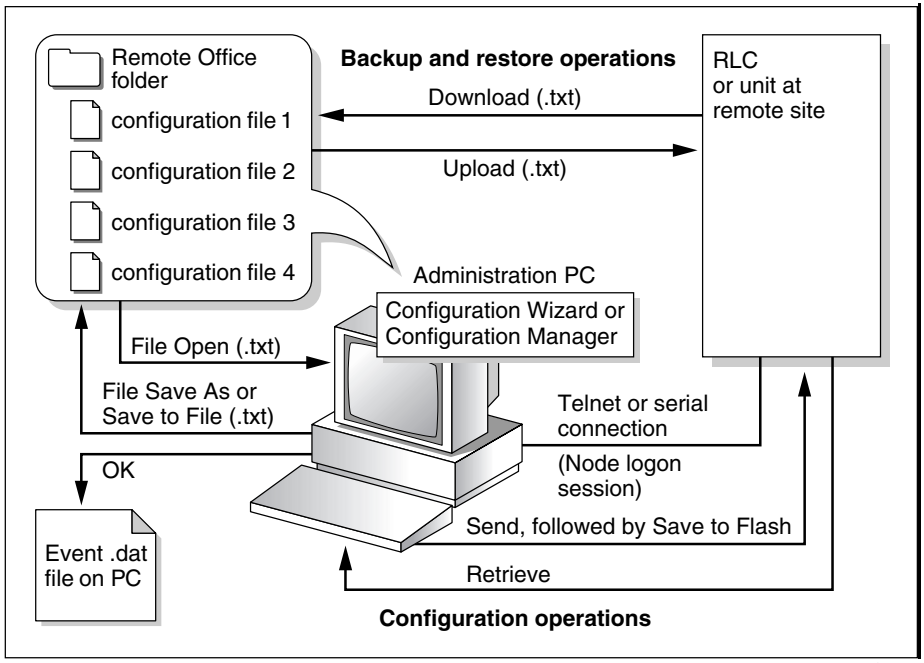
- To refer to a list of Help topics, click on the **Contents** tab.
- To look up a subject alphabetically, click on the **Index** tab.
- To do a full-text search to find topics that contain the words you enter, click on the **Find** tab.

Configuration files description

This section describes configuration files and the ways that 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.



Types of files

You can work with three types of files in Configuration Manager. Each file is identified by one of the file name extensions described in the following table:

File name	File type	When it is created and used
event.dat	Log file	The log (event.dat) 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 of the unit ■ performing configuration changes ■ performing firmware upgrades This file can be very useful when troubleshooting system problems. Technical support personnel may ask for this file. **Note:** Information is appended to this file each time you start a new Configuration Manager session.
*.txt	Text	The text (.txt) file is created when you do one of the following: ■ Click on the **Save to File** button while running the Configuration Wizard. ■ Choose File → Save As from the Menu Bar while working in Configuration Manager. ■ Choose Upload/Download → Download Configuration from the Menu Bar 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 on the **Open** button while running the Configuration Wizard. ■ Choose File → Open from the Menu Bar while running Configuration Manager. ■ Choose Upload/Download → Upload Configuration from the Menu Bar to load the configuration file to the unit's buffer. For more details about these tasks, refer to ■ "Working with configuration files" on page 145 ■ "Creating a backup configuration file" on page 280 ■ "Restoring the configuration" on page 283 **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 the upgrade (.upg) file when performing firmware upgrades. For more details, refer to "Performing a firmware upgrade" on page 288.

Configuration Manager: file operations description

The following table describes each operation shown in the “Configuration Manager: file operations diagram” on page 137.

Operation	Description
OK	When you click on the OK button, the following occurs: ■ Configuration Manager checks any changes you made for errors that, if found, produce an error dialog box. If Configuration Manager displays an error dialog box, make the necessary changes, and then click on the **OK** button again. ■ The changes you make are stored in the event.dat file on your PC. For more information about the event.dat file, refer to “Types of files” on page 138. **Note:** You must click on the OK button after making changes to a property sheet. However, your changes are not yet saved. After clicking on the OK button**,** you can send the changes to the logged on unit’s buffer using a Send or Send All command. You can now update the Flash memory of the logged on unit by performing an Upload/Download → Save to Flash operation from the Menu Bar. For more details, refer to “Send” on page 141. **Note:** If you do not click on the OK button on a property sheet before displaying another property sheet, you lose all of the changes made on the first property sheet. To regain lost changes, you must reenter them.
File → Open	When you choose File → Open from the Menu Bar, 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).

Operation	Description
File → Save As	When you choose File → Save As from the Menu Bar, Configuration Manager saves the unit's configuration to a file on your PC. You must specify the file name and directory location. After saving the file, you can open and modify it at a later time. **Notes:** ■ Configuration Manager saves the file as a text (.txt) file. ■ If you close Configuration Manager without choosing File → Save As, you lose all of the changes you made.
Send	When you click on the Send button, Configuration Manager sends any changes made on the displayed property sheet to the buffer of the logged-on unit. If the send is successful, the following message displays: `Data Sent Successfully` (Nortel Networks recommends that you click on the OK button before clicking on the Send button.) **Note:** You must choose Upload/Download → Save to Flash from the Menu Bar to save the changes to the unit's Flash memory. For more details, refer to "Save to Flash" on page 142.
Send All	When you choose Upload/Download → Send All on any property sheet, changes for *all* property sheets pertaining to the logged-on unit are sent to the buffer on the unit you are connected to. If the send is successful, the following message displays: `Data Sent Successfully` **Note:** You must choose Upload/Download → Save to Flash from the Menu Bar to save the changes to the unit's Flash memory. For more details, refer to "Save to Flash" on page 142.

Operation	Description
Retrieve	When you click on the Retrieve button on a property sheet, the configuration stored in the buffer of the unit that you are connected to (the latest configuration information) displays in Configuration Manager. If the retrieval is successful, the following message displays: `Data Received Successfully`
Save to Flash	When you choose Upload/Download → Save to Flash from the Menu Bar, the information stored in the logged-on unit's buffer is saved to Flash memory. This prevents the configuration from being lost if the unit loses power. While in progress, the following message displays in the status bar at the bottom of the screen: `Save to Flash` When the Save to Flash is completed, the Data Stored to Flash dialog box displays. Some changes require a restart of the unit after saving the changes. If a restart is necessary, Configuration Manager prompts you to do so. **Notes:** ■ You must click on the Send button or choose Upload/ Download → Send All from the Menu Bar *before* you choose Upload/Download → Save to Flash. Perform a Save to Flash as often as you think it is necessary, to keep your configuration information safe. ■ Do not ignore error messages in the Save to Flash process. If Save to Flash fails, retry uploading and saving to Flash. If the problem persists, check the file being uploaded and report the problem to Nortel Networks.

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 active unit. 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` displays in the status bar at the bottom of the screen. When the Save to Flash is completed, the Data Stored to Flash dialog box displays. **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, refer to "Performing a system restart or shutdown" on page 161. ■ If the upload fails or aborts, confirm that you are uploading the correct file. If the problem persists, contact Nortel Networks technical support for assistance.

Operation	Description
Download Configuration	When you choose Upload/Download → Download Configuration from the Menu Bar, Configuration Manager saves the configuration stored on the logged-on unit 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. If you make changes and do not save them, you lose those changes.

Working with configuration files

This section explains how to:

- create a configuration file (refer to page 146)
- open a configuration file in Configuration Manager (refer to page 146)
- perform a configuration upload (refer to page 147)
- perform a configuration download (refer to page 147)

When to use 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 logged on to a unit, the file save operation is optional. To save the configuration to Flash, first update the unit's local buffer by clicking on the Send button or choosing Upload/Download → Send All from the Menu Bar. Then, use Upload/Download → Save to Flash to complete the operation.
■ Send ■ Send All ■ Retrieve ■ Upload Configuration ■ Download Configuration	connected and logged on to a unit.

Creating a configuration file on the PC

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 can perform an *offline configuration.*
3. From the Menu Bar, choose File → Save As.

   Result: The Save As dialog box displays.
4. Enter a descriptive name for the file.

   The file name normally identifies the type of configuration it contains.

   Example 1: If the file contains a basic configuration that is to be used for a specific type of unit, enter **template** as the file name.

   Example 2: If the file contains a configuration that is unique to a specific unit, enter the unit's name or number as the file name.
5. Ensure that the Save as type drop down box shows text file (*.txt)
6. Specify the folder where you want to save the file.
7. Click on the **OK** button.

   Result: The file is saved.

   Note: Nortel Networks strongly recommends that you do not manually edit this file.

Opening a configuration file

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 Bar, choose File → Open.

   Result: The Open dialog box displays.
4. Ensure the Files of type drop down box shows text files (*.txt).

5 Navigate to the folder containing the file you need.

6 Select the file, and then click on the **Open** button.

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

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

8 Make changes as necessary, then complete the following actions:

a. Save the file by choosing File → Save from the Menu Bar. If you want to change the file name, choose File → Save As from the Menu Bar.

b. Click on the **Send** button to update the unit, then choose Upload/ Download → Save to Flash from the Menu Bar.

Uploading a configuration to a unit

For complete instructions on uploading a configuration to a unit, refer to "Restoring the configuration" on page 241.

Downloading a configuration from a unit

For complete instructions on downloading a configuration to a unit, refer to "Creating a backup configuration file" on page 238.

Selecting the device type for offline configuration

If you are not logged on to a Remote Office unit (that is, an RLC, Remote Office 9150 unit, a Remote Office 911x series unit, or a Meridian Digital Telephone IP Adapter unit), then you must select the device type you want to work with. Configuration Manager reorganizes the system tree with the property sheets associated with that device type.

Note: When working with a Meridian Digital Telephone IP Adapter unit in Configuration Manager, use Remote Office 911x property sheets.

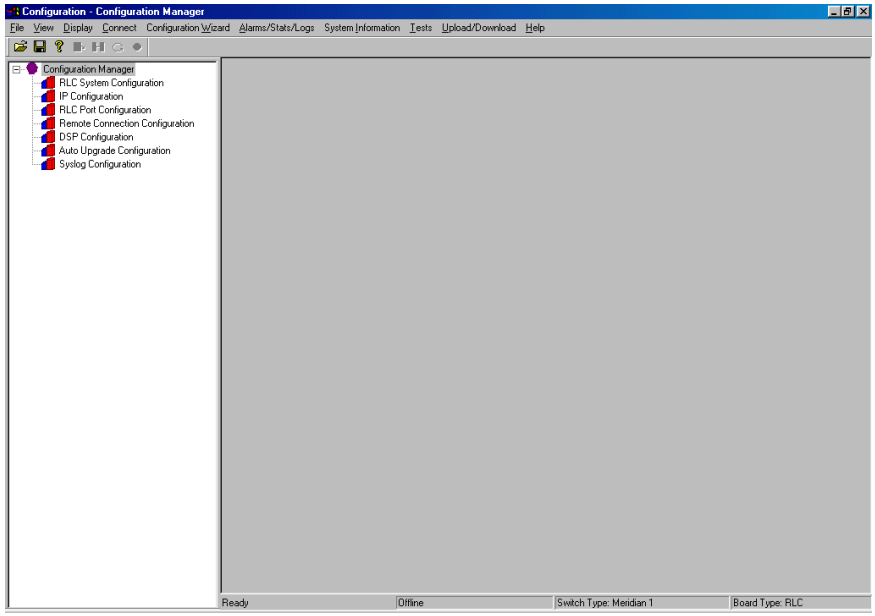
To select the device type for offline configuration:

1 Start Configuration Manager as described in “What is Configuration Manager?” on page 126.

2 From the Menu Bar, choose View → Device Type, and the type of device (for example, RLC, 9150, 911x).

3 Click on the plus (**+**) sign beside Configuration Manager in the left pane.

Result: The system tree expands in the right pane, similar to the following:



Logging on to a unit

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 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 RLC or Remote Office 9150 unit, you can establish an IP connection with Telnet.

Default logon ID and password

The default logon ID is **guest**. You cannot change the logon ID.

The default password is **guest123**. The password can be changed and, therefore, can be different if this is not a first time installation. Nortel Networks recommends that you do not change the password until your Remote Office system is up and running smoothly.

Connection history

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

Note: Upgrading the Configuration Manager software deletes the connection history list.

Auto logoff

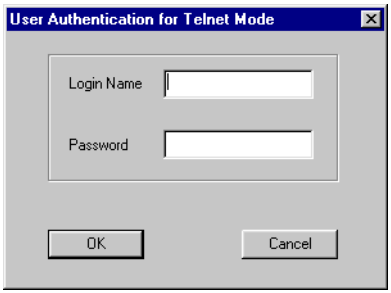
If the connection remains open with no activity for 15 minutes, then Configuration Manager automatically logs off the connection and the Session Timed Out message displays. This helps to secure the configuration in the event that you walk away from the administration PC while logged on to a unit.

Logging on to a unit using the connection history

To log on to a unit using the connection history:

1 From the Menu Bar, choose Connect → XXX.XXX.XXX.XXX (IP address of the unit you want to log on to).

Result: If no one else logged on to the unit before you and if IP connectivity exists to this unit, the User Authentication for Telnet Mode dialog box displays. It is similar to the following:

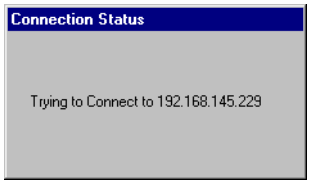


2 Enter your logon name in the Login Name field. If you have not yet customized this setting, refer to “Default logon ID and password” on page 149 for the default logon ID.

3 Enter your password in the Password field. If you have not yet customized this setting, refer to “Default logon ID and password” on page 149 for the default password.

4 Click on the **OK** button.

Result: Configuration Manager initiates a connection attempt. The Connection Status message box displays. It is similar to the following:

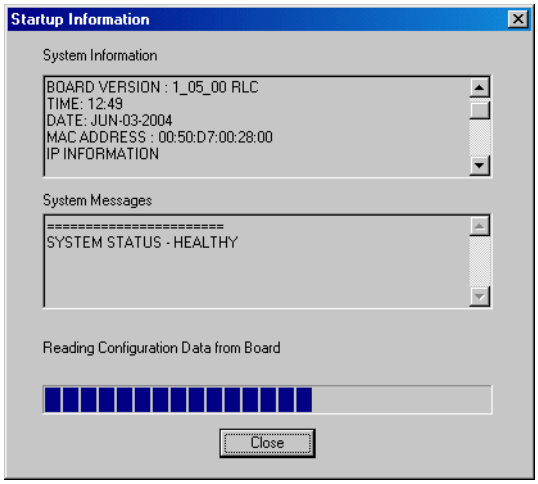


Note: The connection speed can be too fast for this message to be seen in a successful logon attempt.

If you do not enter any logon information, after two minutes Configuration Manager displays a reminder dialog box similar to the following:

Click on the **OK** button to return to Step 2 on page 150.

IF the logon attempt	THEN
fails,	a message box similar to the following displays:  Complete the following actions: 1 Click on the **OK** button. 2 Go back to Step 1 on page 150 to try again.

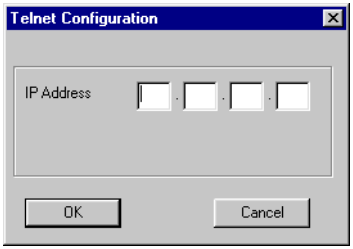
IF the logon attempt	THEN
is successful,	the User Logged In dialog box displays. Click on the **OK** button. **Result:** The Startup Information dialog box displays. It is similar to the following:  Messages display above the progress bar at the bottom of the dialog box, similar to the following: ■ `Reading Hardware Information` ■ `Reading DSP Load Data` ■ `Reading Configuration Data` These messages mean that Configuration Manager is obtaining the unit's configuration information from Flash memory. When initialization is complete, the `Configuration Data Read Successfully` message displays above the progress bar. Click on the **Close** button.

Logging on to a unit using Telnet

To log on to a unit using Telnet:

1 From the Menu Bar, choose Connect → Logon Unit → Telnet.

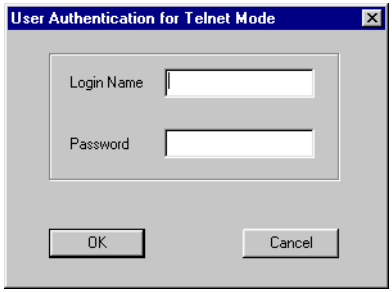
Result: The Telnet Configuration dialog box displays, similar to the following:



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

3 Click on the **OK** button.

Result: If no one else logged on to the unit before you, and if IP connectivity exists to this unit, the User Authentication for Telnet Mode dialog box displays, similar to the following:

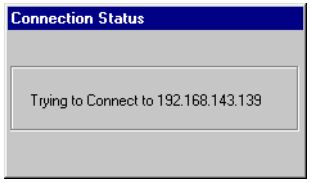


4 Enter your logon name in the Login Name field. If you have not yet customized this setting, refer to “Default logon ID and password” on page 149 for the default logon ID.

5 Enter your password in the Password field. If you have not yet customized this setting, refer to “Default logon ID and password” on page 149 for the default password.

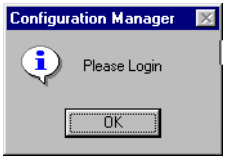
6 Click on the **OK** button.

Result: Configuration Manager initiates a connection attempt. The Connection Status message box displays. It is similar to the following:



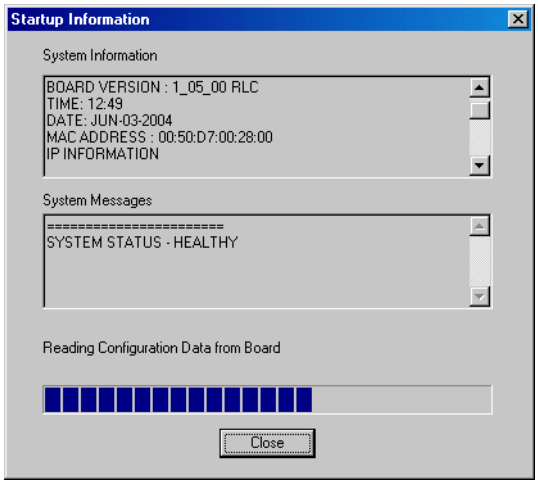
Note: The connection speed can be too fast for this message to be seen in a successful logon attempt.

If you do not enter any logon information, after two minutes Configuration Manager displays a reminder dialog box similar to the following:



Click on the **OK** button to return to Step 4 on page 153.

IF the logon attempt	THEN
fails,	a message box similar to the following displays:  Complete the following actions: 1 Click on the **OK** button. 2 Go back to Step 1 on page 153 to try again.

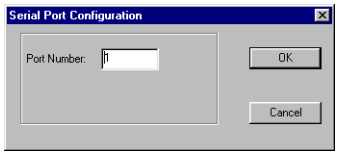
IF the logon attempt	THEN
is successful,	the User Logged In dialog box displays. Click on the **OK** button. **Result:** The Startup Information dialog box displays. It is similar to the following:  Messages display above the progress bar at the bottom of the dialog box, similar to the following: ■ `Reading Hardware Information` ■ `Reading DSP Load Data` ■ `Reading Configuration Data` These messages mean that Configuration Manager is obtaining the unit's configuration information from Flash memory. When initialization is complete, the `Configuration Data Read Successfully` message displays above the progress bar. Click on the **Close** button.

Logging on to a unit using the serial port

To log on to a unit using the serial port:

1 From the Menu Bar, choose Connect → Logon Unit → Serial.

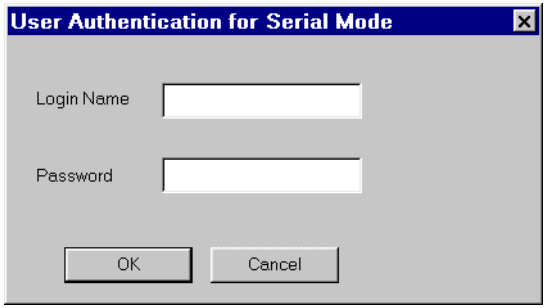
Result: The Serial Port Configuration dialog box displays, similar to the following:



2 Enter the COM port number the unit is connected to in the Port Number field.

3 Click on the **OK** button.

Result: If no one else logged on to the unit before and if your PC is connected with a serial cable to the RLC, the User Authentication for Serial Mode dialog box displays. It is similar to the following:



4 Enter your logon name in the Login Name field. Refer to “Default logon ID and password” on page 149 for the default logon ID if you have not yet customized this setting.

5 Enter your password in the Password field. Refer to “Default logon ID and password” on page 149 for the default password if you have not yet customized this setting.

6 Click on the **OK** button.

Result: The connection attempt is initiated. The following message might display:

```
Trying to Connect via Serial Port <port number>
```

IF the logon attempt	THEN
fails,	the following message displays: `SERIAL CONNECTION FAILED` Check the serial port connection and ensure it is good. Then, go back to step 1.
is successful,	the User Logged In dialog box displays. Click on the **OK** button. **Result:** The Startup Information dialog box displays. Messages display above the progress bar at the bottom of the dialog box, similar to the following: ■ `Reading Hardware Information` ■ `Reading DSP Load Data` ■ `Reading Configuration Data` These messages mean that Configuration Manager is obtaining the unit's configuration information from Flash memory. When initialization is complete, the `Configuration Data Read Successfully` message displays above the progress bar. Click on the **Close** button.

Logging off of the unit

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

To log off of the unit:

1 From the Menu Bar, choose Connect → Logoff Unit.

Result: The Log off dialog box displays, similar to the following:

2 Click on the **Yes** button.

Result: The Configuration Manager: User Logged off dialog box displays, similar to the following:

3 Click on the **OK** button.

Using the Remote Connection command

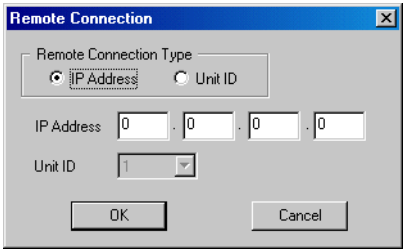
Use the Remote Connection command to log on to multiple Remote Office units during a single Configuration Manager session.

Note: Configuration Manager does not allow multiple users to log on to the same Remote Office unit simultaneously. To allow subsequent users to log on at a later time, you must log off of all Remote Office units that you have accessed before ending your Configuration Manager session.

The Remote Connection command allows you to move between Remote Office units without logging off from the current unit before logging on to another unit. After you log on to one unit using the Connect → Logon Unit command, log on to another unit using the following procedure:

1 From the menu, choose Connect → Remote Connection.

Result: The Remote Connection dialog box displays, similar to the following:



2 Do one of the following:

- Click on the **IP Address** option button if you want to connect to the unit through the IP address.

  Note: This option is available when you are logged on to any Remote Office unit.

- Click on the **Unit ID** option button if you want to connect to the unit through the Unit ID.

  Note: This option is only available when you are logged on to an RLC. Use this option when accessing a Remote Office unit located behind a NAT router or Firewall device.

3 Do one of the following:

- Enter the IP address of the unit that you want to connect to in the IP Address fields.

  Note: This option is available when you are logged on to any Remote Office unit.

- Enter the unit ID of the unit that you want to connect to in the Unit ID field.

  Note: This option is only available when you are logged on to an RLC. Use this option when accessing a Remote Office unit located behind a NAT router or Firewall device.

4 Click on the **OK** button.

Result: Configuration Manager initiates a connection attempt. The following message can appear:

```
Trying to Connect to <IP address> or <unit ID>
```

Refer to “Logging on to a unit” on page 149 for more information.

When you complete your work on a unit, you must log off from that unit. Execute a Connect → Logoff Unit command for each unit that you logged on to before ending your Configuration Manager session.

Performing a system restart or shutdown

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

When to perform a restart or shutdown

Each time that you make a configuration change, perform a Save to Flash. You must also restart the unit if Configuration Manager prompts you to do so.

Note: When you save configuration changes to Flash, the system suspends new call processing for approximately 30 seconds. Some configuration changes do not take effect until the unit has been re-started.

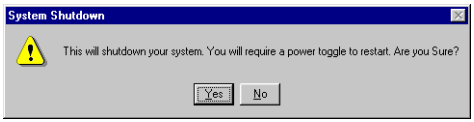
You can perform a system shutdown when you need to power the system down.

Performing a system restart

To perform a system restart:

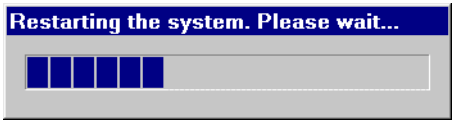
1 From the Menu Bar, choose Connect → System Reset → Restart.

Result: The System Restart dialog box displays, similar to the following:



2 Click on the **Yes** button.

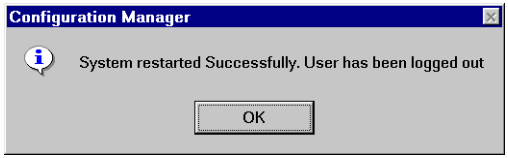
Result: The following status dialog box displays:



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

```
Restarting the System
```

The status continues to show Online. When the system restart is complete, a dialog box displays informing you that the system restart was successful, and that you are logged off, similar to the following:



3 Click on the **OK** button.

Result: Configuration Manager prompts you to log back on using the previous connection method (Serial or Telnet).

Performing a system shutdown

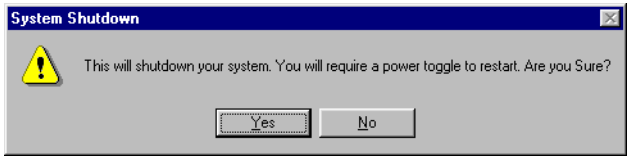
ATTENTION

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

To perform a system shutdown:

1 From the Menu Bar, choose Connect → System Reset → Shutdown.

Result: The System Shutdown dialog box displays, similar to the following:



2 Click on the **Yes** button.

Result: Configuration Manager disconnects your logon session and the following message displays in the status bar at the bottom of the screen:

```
Shutting Down the System
```

The status shows Offline.

3 Turn the power on the Remote Office unit off.

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

Closing Configuration Manager

When you have completed all of the configuration modifications you want to make, or are done viewing unit logs and statistics, log off and 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.

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.

To close Configuration Manager:

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

- From the Menu Bar, choose File → Save As, 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 you are connected to by doing one of the following:
  - — Click on the **Send** button on any property sheet, then choose Upload/Download → Save to Flash from the Menu Bar.
  - — Click on the **Send All** button on any property sheet, then choose Upload/Download → Save to Flash from the Menu Bar.
  - — If you have saved the changes to a file, choose Upload/Download → Upload Configuration from the Menu Bar. For instructions, refer to "Restoring the configuration" on page 241.

2 Log off by choosing Connect → Logoff Unit from the Menu Bar.

3 Choose File → Exit from the Menu Bar.

Result: Configuration Manager closes.

Uninstalling the Configuration Manager software

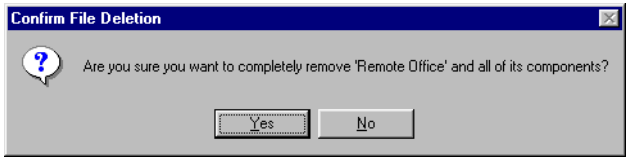
To remove the Configuration Manager software from your administration PC:

1 Choose Start → Settings → Control Panel.

2 Double-click on the **Add/Remove Programs** icon.

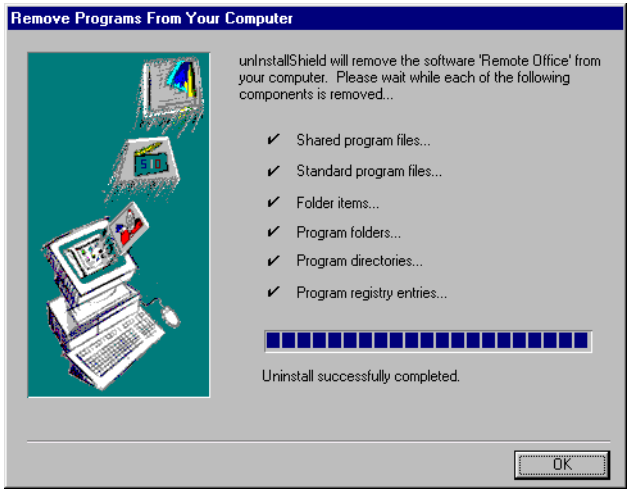
3 Select Remote Office from the list, and then click on the **Add/Remove** button.

Result: The Confirm File Deletion dialog box displays, similar to the following:



4 Click on the **Yes** button.

Result: The Uninstall Shield begins the uninstall and displays the uninstall progress. When the uninstall is completed, the screen displays as follows:



Chapter 6

Configuring the RLC

In this chapter

Using the XConnect command for PBX maintenance from a remote site

Use the XConnect command to establish a connection to the host PBX's serial data interface (SDI) port from a remote site. First, you must ensure that there is a straight-through serial connection from the RLC to the PBX's SDI port. Then, you must log on to the RLC using Telnet. With these connections established, remote-site system administrators can perform PBX maintenance procedures.

Notes:

1. The terminal settings must be as follows: 9600 8 N 1 (9600 Baud, 8 data bits, No parity, 1 stop bit).
2. The XConnect command requires that you connect plug 2 of the RLC Multi-I/O cable (Basic or Enhanced) to the PBX's SDI port.

Getting there RLC → Configuration Manager

Connecting to the host PBX's SDI port from a remote site

To connect to the host PBX's SDI port from a remote site:

1 Log on to the RLC using Telnet.

2 Choose Connect → XConnect from the Menu Bar.

Result: Configuration Manager warns you that if you continue with an SDI session, ending that session logs you off of the logged-on unit.

3 Click on the **Yes** button.

Result: Configuration Manager establishes the serial connection from the RLC to the host PBX's SDI port and presents you with the XConnect log screen.

4 Conduct the required PBX maintenance activities.

5 Click on the **Close** button to end your PBX configuration session.

Result: Configuration Manger closes the serial connection to the host PBX's SDI port and logs you off of the RLC.

Note: If you want to resume your connection to a specific unit, you must use the Connect → Logon Unit command to re-establish the connection.

RLC system configuration

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

1. General Configuration – Identify this RLC within your remote network and address voice quality and signal strength issues at the remote site. In addition, this category allows you to configure Trunk Support according to the speed of your connection.
2. IDVR Feature – The Integrated Digital Voice Recorder (IDVR) is a TelStrat product. For information on configuring IDVR functionality, contact your TelStrat representative.
3. DN Discovery Schedule – Set the times when the RLC automatically determines the name and number assigned to the all line keys on each RLC remote port.

Voice Activity Detection

Enable Voice Activity Detection (VAD) to prevent packet transmission during periods when there is no voice data present. This can help you to save bandwidth. To enable VAD, click on the **Enable** option button under Voice Activity Detection.

If you are having difficulties with voice quality, see if silence suppression has an effect on the problem by disabling VAD. To disable VAD, click on the **Disable** option button under Voice Activity Detection.

Note: When using the bandwidth rules described on the Bandwidth usage table in the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103), use the Peak Rate to calculate IP bandwidth overhead if VAD is disabled. Allocate additional bandwidth over the ISDN for PSTN connections between the RLC and the Remote Office 9150 unit, including QoS transition. When you enable VAD, the amount of bandwidth allocation is 120% of the normal rate. Therefore, if you use G.729A, the bandwidth allocation is 9.6K instead of 8K. If you use G.726, the bandwidth allocation is 38.4K instead of 32K. If the available bandwidth over the PSTN is insufficient, the call is blocked and you receive a message indicating insufficient bandwidth.

Jitter Buffer target depth

The RLC's dynamic voice jitter attenuation buffer compensates for the uneven arrival of voice packets across data networks. This buffer collects packets that arrive unevenly and relays them evenly.

Select the size of the buffer in the Jitter Buffer drop down box. The valid options are 30, 60, and 90 milliseconds (ms).

Configure the jitter buffer according to the following guidelines when upgrading to Remote Office product release 1.5:

- high-speed (>T1 connections) or LANs — leave at the default
- medium-speed (for example, fractional T1s with speeds of greater than 128K) — set to 60 milliseconds
- low-speed (64K or ISDN) or high-data environments — configure at 90 milliseconds. This is especially true if using G.711.

Advanced configuration settings

Click on the **Advanced Configuration** button to access the Advanced Configuration dialog box. This dialog box provides access to the following fields:

Field	Description
Dialtone/DTMF Relay	■ Click on the **Enable** option button to instruct the RLC and its remote units to send the dial tone and DTMF tones as data packets. ■ Click on the **Disable** option button to instruct the RLC and its remote units to send the dial tone and DTMF tones as voice packets. The default is Enable.
NLP (Non-Linear Processing)	Refer to "NLP" on page 170 for information on the proper configuration of NLP settings.

Dialtone/DTMF Relay

Dialtone/DTMF Relay allows you to manage the bandwidth used by your Meridian units for generating dial tone and Dual Tone Multi-Frequency (DTMF), or button-press, tones. With Dialtone/DTMF Relay enabled, Meridian units send encoded data packets to the other side when they detect either dial tone or DTMF tones. With Dialtone/DTMF Relay disabled, the units send voice packets to the other side when they detect a dial tone or DTMF tones. The former method uses less bandwidth, but produces rougher DTMF tones and a dial tone that begins with an audible click. The latter method produces smoother DTMF tones and dial tone, but uses more bandwidth.

NLP

The non-linear processor (NLP) works with the Remote Office echo canceller to reduce echo. Echo occurs in a telephone call when the transmitted signal reflects and is received by the transmitting device. To cancel the echo, the Remote Office system monitors the audio stream looking for echo. When echo is identified it is digitally (mathematically) removed. If the echo is very strong, a small amount of echo may remain called "residual" echo. The aggressiveness of the NLP determines how quickly and how effectively the Remote Office NLP reduces the residual echo.

The operation of the NLP can affect how the audio sounds during double-talk situations - when both parties are speaking. Cultural differences also changes how often double-talk occurs during a conversation.

Nortel Networks recommends the following settings as a starting point:

- RLC: NLP Enabled - Less Aggressive (default)
- 9150: NLP Enabled - More Aggressive (default)

If the Remote Office 9150 unit user hears echo during conversations, adjust the settings, as follows:

- RLC: NLP Enabled - More Aggressive
- 9150: NLP Enabled - Less Aggressive

If the party on the PBX side hears echo during conversations, adjust the settings, as follows:

- RLC: NLP Enabled - More Aggressive
- 9150: NLP Enabled - More Aggressive

The NLP does not have to operate aggressively if echo is not present. If echo is not present but double-talk is present, even with Less Aggressive settings, try disabling the NLP on the RLC.

DN Discovery

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

Some of the characteristics of DN Discovery are:

- DN Discovery overrides the DN configuration for Local Call keys.
- Local SwitchOver and Bridge Ports require DN Discovery.
- The Remote Office 9150 unit also uses the discovered DNs to determine when it can switch calls locally.
- MADN appearances of the DN Discovery port ring periodically during DN Discovery.To avoid this, do not start DN Discovery more frequently than once per half-hour and add a unique SCR key for DN Discovery.
- If Make Set Busy is active, DN Discovery fails and results in blank DN displays on M39xx sets. To avoid this, do not activate Make Set Busy for the port designated for DN Discovery.
- For DN Discovery to work using key 0 on the target port, no special Class of Service (CLS) is required. If the target key is key 1 or higher, TDD CLS is required.
- The target key must be a Single Call Ringing (SCR) or Multiple Call Ringing (MCR) key - not an ACD key.

DN Discovery configures the DNs for the local call keys based upon the first line key DN discovered in the PBX configuration of the RLC port. Therefore, the first line key DN must be unique on all sets.

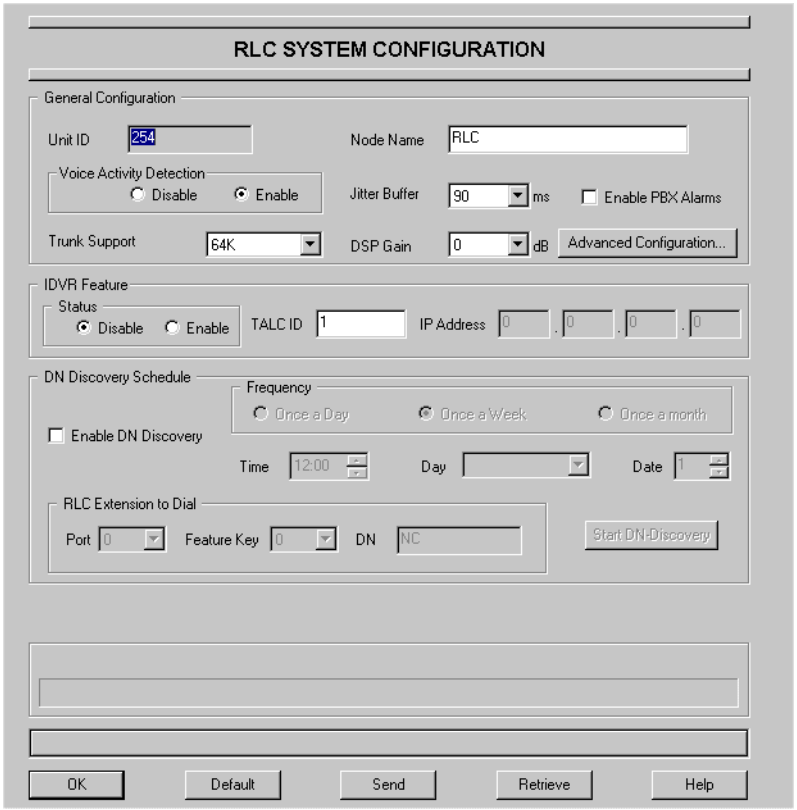
How it works

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

The host PBX regularly provides updated keymaps of the remote station's feature keys to the RLC. For each feature key configured as a line key, the RLC places a call. For each call, the host PBX produces Calling Line Identification (CLID) information revealing the primary DN of the remote port the call is placed to.

Getting there RLC → Configuration Manager → RLC System Configuration

RLC System Configuration property sheet



Configuring the RLC system information

To configure the RLC system information:

1 Complete the fields as described in “RLC System Configuration field descriptions” on page 174.

2 Click on the **OK** button

Result: Configuration Manager writes the changes to a temporary file on the administration PC.

3 Click on the Send button to update the RLC with the new information.

Notes:

a. To save changes to the RLC’s Flash memory, select Upload → Save to Flash from the Menu Bar.

b. When you change System configuration parameters and Save to Flash, calls can be dropped. Ensure that there are no active calls when you make changes to these parameters.

RLC System Configuration field descriptions

Field	Description
Unit ID	The Unit ID is always set as 254. The remote units in a Remote Office system must have Unit IDs unique among all units connected to the same RLC. **Note:** This Unit ID must also be entered on the RLC Connection Configuration property sheet pertaining to each remote unit. With this information, the system creates the communication path between the remote unit and this RLC.
Node Name	Enter a descriptive name for this RLC.
Voice Activity Detection	■ Click on the **Disable** option button if you do not want the RLC to stop sending voice packets across the network when no one is speaking. ■ Click on the **Enable** option button if you want the RLC to stop sending voice packets across the network when no one is speaking. The default is Enable.
Jitter Buffer	Select the length of time, in milliseconds (ms), that you want the RLC to collect unevenly arriving voice packets so that it can relay them evenly. This action works to minimize audible jitter. Valid options are 30, 60 and 90 ms. The default is 90 ms.
Enable PBX Alarms	Click on the **Enable PBX Alarms** checkbox if you want the RLC to notify the host PBX to produce alarms and alerts. If you don't want the RLC to notify the host PBX to produce alarms and alerts, ensure that the Enable PBX Alarms checkbox is not selected. Refer to “Display Logs” in Configuration Manager online Help to determine which alarms and alerts the PBX generates.

Field	Description
Advanced Configuration	Click on the **Advanced Configuration** button to display the Advanced Configuration dialog box. From this dialog box, you can to configure the following settings for the RLC: ■ Dialtone/DTMF Relay to configure whether the PBX or the Remote Office unit generates the dial tone and DTMF (button-press) tones ■ Non-Linear Processing (NLP) to configure echo cancellation settings for calls supported by your Remote Office system For more information, refer to "Advanced configuration settings" on page 169.
Trunk Support	Configure the speed of your Remote Office connection as follows: ■ Choose **56K** if the speed of your Remote Office connection is 56 Kbps. ■ Choose **64K** if the speed of your Remote Office connection is 64 Kbps. ■ Choose **Dynamic** if your Remote Office connection includes speeds at 56 Kbps and 64 Kbps. **Note:** You must configure the same BRI speed (such as 56K, 64K, or dynamic) on both the RLC and the Remote Office 9150 unit. The default is 64K.
DSP Gain	Select the number of decibels (dB) that you want to add to, or subtract from, the strength of the transmitted signal before the DSP processes it. Valid options are 9, 6, 3, 0, -3, -6, -9, -12, and -15. The default is 0 dB. **Note:** Change this setting at the Host site to address a problem with signal strength at the remote site.

Field	Description
TALC ID	
Status: Disable **Status: Enable**	Refer to page 168 for information on the Integrated Digital Voice Recorder (IDVR).
IP Address	
Enable DN Discovery	Click in the **Enable DN Discovery** checkbox if you want the RLC to automatically detect the PBX-configured name and number assigned to each line key for each remote port on the RLC. If you don't want the RLC to perform DN Discovery, ensure that the Enable DN Discovery checkbox is not selected. **Notes:** **1.** For DN Discovery to work on any key other than key 0,you must enable TDD class of service on the host PBX. **2.** The target key must be a Single Call Ringing (SCR) or Multiple Call Ringing (MCR) key, not an ACD key.
Frequency	Click on the option button that identifies how often you want the RLC to perform DN Discovery: ■ Once a Day ■ Once a Week ■ Once a month
Time	Select the time of day that you want the RLC to perform DN Discovery.
Day	Select the day when you want DN Discovery to be performed (if you selected "Once a Week" in the Frequency field).
Date	Select the date when you want DN Discovery to be performed (if you selected “Once a month” in the Frequency field).

Field	Description
RLC Extension to Dial	Use these fields to configure the port number, feature key position, and DN of the RLC extension to be used for DN Discovery. At the time configured for DN Discovery, each remote port on the RLC places a call to the extension described by these fields. The RLC assigns the incoming Calling Line Identification (CLID) name and number to the calling port: ■ Port – This field identifies the port called for DN Discovery. **Note:** Nortel Networks recommends that you run DN Discovery on an unused port, such as a data port, configured with voice capability. For information on completing this configuration, refer to the port configuration section of the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215). ■ Feature Key – This field identifies the feature key configured on the host PBX for the port called for DN Discovery. ■ DN – This field identifies the DN assigned to the feature key and port called for DN Discovery.
Start DN Discovery	Click on the **Start DN Discovery** button to perform an unscheduled DN Discovery. **Note:** Start DN Discovery is available (not dimmed) only if the configuration in the RLC's Flash memory is the same as the configuration at the local site, and if the Enable DN Discovery checkbox is selected.

Understanding the IP interface

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

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

These items provide the network connection between the RLC, an administration terminal, and the remote site to allow the following to take place:

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

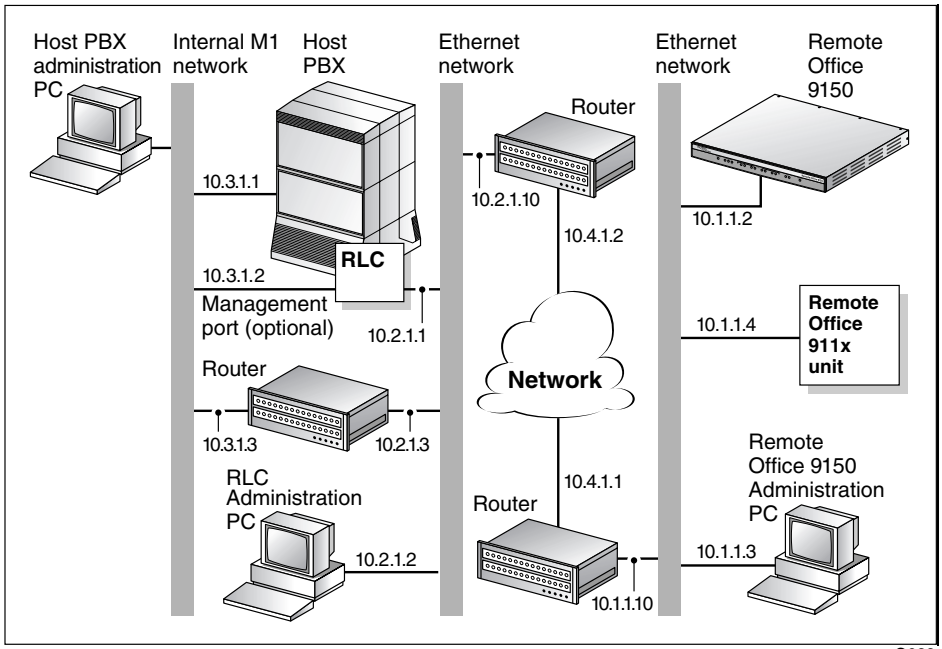
  Once connected, you can view or work with the system configuration.

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

In addition to the IP address, subnet mask, and default gateway mentioned above, you can also assign an IP address to the management port on the RLC. Once you assign this IP address, you can use the PBX administration PC to log on to and administer the RLC through the host PBX's internal network.

Reach Line Card position in your IP network

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



IP configuration

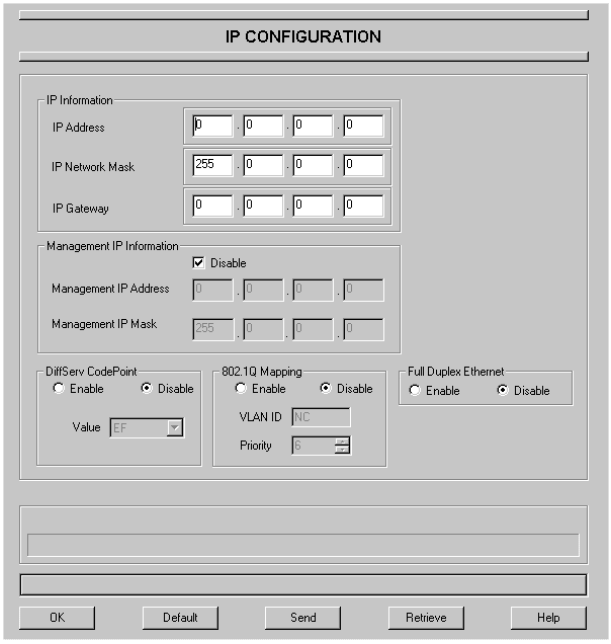
Configure the RLC's IP connectivity on the IP Configuration property sheet. This section explains how to enter the following information:

- the IP address, subnet mask, and default gateway for the primary RLC Ethernet port
- the IP address for the Management RLC Ethernet port used for PBX maintenance over Ethernet
- prioritization of voice packets on the IP network
- prioritization of voice packets on the LANs and WANS

For a description of each of these items, refer to "IP configuration" on page 180.

Getting there RLC → Configuration Manager → IP Configuration

IP Configuration property sheet



Configuring the IP addresses

To configure the IP addresses:

1 Complete the fields as described in “IP Configuration field descriptions” on page 182.

2 Click on the **OK** button.

Result: Configuration Manager writes the changes to a temporary file on the administration PC.

3 Click on the **Send** button to update the RLC with the new information.

Notes:

a. When you change IP configuration parameters and Save to Flash, calls can be dropped. Ensure that there are no active calls when you make changes to these parameters.

b. To save changes to Flash memory, select Upload → Save to Flash from the Menu Bar.

IP Configuration field descriptions

Field	Description
IP Address	Enter the IP address of the RLC.
IP Network Mask	Enter the IP network mask of the RLC.
IP Gateway	Enter the IP gateway of the RLC.
Management IP Information	■ Click in the **Enable** check box if you want to assign an IP address on the host PBX's internal LAN to the RLC. **Result:** The check box clears and Configuration Manager enables the Management IP Address and Management IP Mask fields. ■ Click in the **Disable** check box if you do not want to assign an IP address on the host PBX's internal LAN to the RLC. Since this is the default setting, you only need to do this after you have enabled management IP information. **Note:** The second Ethernet port of the RLC is only available with the RLC Multi-I/O cable–Enhanced.
Management IP Address	Enter the IP address of the RLC on the host PBX's internal LAN.
Management IP Mask	Enter the IP network mask of the host PBX if you want remote units connected to this RLC to have the ability to configure PBX settings.

Field	Description
DiffServ CodePoint	This setting modifies the IP Header and is applicable across the entire WAN. If enabled, this feature allows you to set the DiffServ CodePoint value. Refer to the "DiffServ CodePoint: Value" for a list of values. ■ Click on the **Enable** option button if you want to allow prioritization of voice packets sent from this RLC over WAN portions of the network. ■ Click on the **Disable** option button if you do not want to allow prioritization of voice packets sent from this RLC over WAN portions of the network. The default is Disable.
DiffServ CodePoint: Value	Select the DiffServ CodePoint value from the drop down box. Valid options and their value (in hexadecimal) are: ■ CS7 (Precedence 7 - Network Control) - 0x38 ■ CS6 (Precedence 6 - Inter-network Control) - 0x30 ■ EF (Expedited Forwarding) - 0x2E ■ AF41 (Assured Forwarding Class 4, Delay = Normal, Throughput = High, Reliability = Normal) - 0x22 ■ AF31 (Assured Forwarding Class 3, Delay = Normal, Throughput = High, Reliability = Normal) - 0x1A ■ AF21 (Assured Forwarding Class 2, Delay = Normal, Throughput = High, Reliability = Normal) - 0x12 ■ AF11 (Assured Forwarding Class 1, Delay = Normal, Throughput = High, Reliability = Normal) - 0x0A ■ DE (Default) - 0x00 The default is EF.

Field	Description
802.1Q Mapping	This setting inserts an additional tag at the Media Access Control (MAC) layer of IEEE 802.3 and therefore ends at the first router. Refer to RFC 2474. ■ Click on the **Enable** option button if you want to allow prioritization of voice packets sent from this RLC over LAN portions of the network. ■ Click on the **Disable** option button if you do not want to allow prioritization of voice packets sent from this RLC over LAN portions of the network. The default is Disable.
802.1Q Mapping: VLAN ID	Enter the Virtual Local Area Network (VLAN) ID for 802.1Q Mapping. Valid entries are 0 through 4094 (0xFFE) and NC (Not Configured). The default is NC.
802.1Q Mapping: Priority	Select the priority value for 802.1Q Mapping from the Priority scroll box. Valid options are 0 through 7. The default is 6.

Field	Description
Full Duplex Ethernet	This setting configures Ethernet support on the RLC to allow simultaneous transmission and reception of Ethernet packets. When you enable full-duplex Ethernet, you must also set the corresponding port on the connected switch, hub, or router to 10 FULL Duplex. Remote Office products do not support Auto negotiation of the Ethernet interface. ■ Click on the **Enable** option button if you want to allow 10-Megabit per second transmission in both directions, send and receive. ■ Click on the **Disable** option button if you do not want to allow 10-Megabit per second transmission in both directions, send and receive. The default is Disable. **Note:** When you configure a full-duplex Ethernet connection, the RLC's Ethernet collision LED remains on solid (constantly lit).

Prioritizing voice traffic over shared networks

Prioritizing voice traffic on shared networks can improve QoS on LAN and WAN segments of the network that support prioritization. Achieving the desired QoS through prioritization over LAN connections requires you to enable 802.1Q Mapping. Achieving the desired QoS through prioritization over WAN connections requires you to enable the DiffServ CodePoint.

For more information on DiffServ, 802.1Q, and quality of service in general, refer to “Evaluating your network”, and “Quality of service issues” in the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103).

RLC port configuration

Ports on the RLC can be configured as one of the following ports:

- Remote ports provide host-PBX access to a remote user station. Configure at least one Remote port for each remote unit (Remote Office 9150, 9115, 9110 unit, or Meridian Digital Telephone IP Adapter) and for each Bridge port configured on a Remote Office 9150 unit.

  Note: Bridge ports, configured on Remote Office 9150 units, allow the 9150 unit to give incoming, local, PSTN calls access to the following PBX features: Transfer, Call Forward, and Conference.

- Network ports establish PSTN connections between the RLC and its remote units.

  Note: A common mistake in programming a PSTN connection is to enable only a single port (typically Port 16) on the RLC. Keep in mind, that one port must be programmed for each ISDN call that the Remote Office 9150 unit can place to the PBX. Note that typically a BRI line from a CO has the capability of placing two ISDN calls (2 B-channels) and therefore would require two network ports to be configured on the RLC. Refer to the PBX configuration notes for Class of Service requirements.

- Local ports provide local digital telephone connections directly to the RLC.

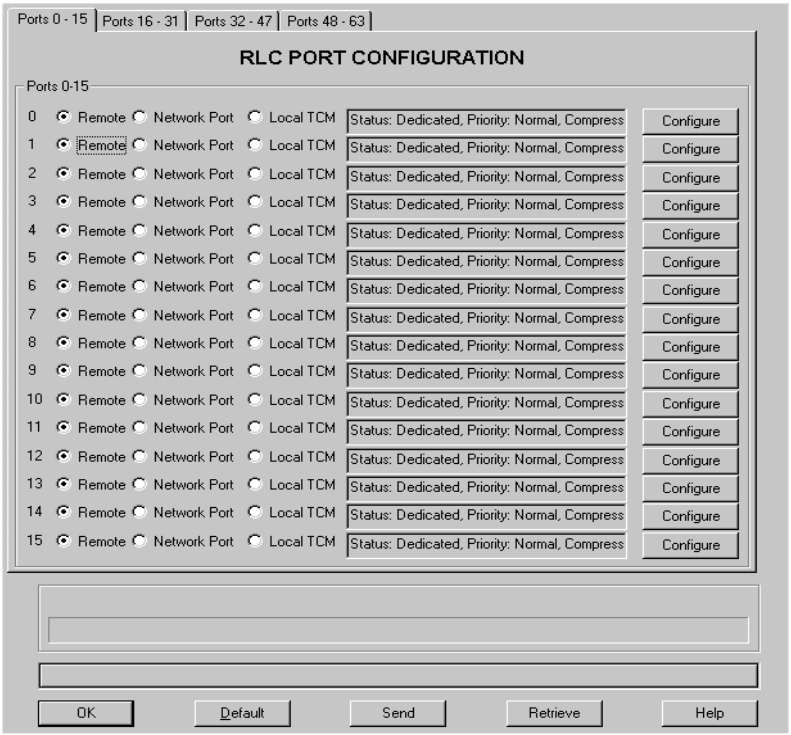
The following table describes port number ranges and how they can be configured.

Ports	can be assigned to
0 through 15 and 32 through 47	digital telephone sets that are assigned to remote users. **Note:** The associated ports on the host PBX must be configured with voice capability.

Ports	can be assigned to
16 through 31 and 48 through 63	■ stations equipped with ATAs or MCAs **Note:** For ATA and MCA compatibility with Remote Office 911x series units, refer to "Network port configuration" on page 116. ■ network ports for configuring a trunk between the RLC and a remote unit. **Note:** The associated ports on the host PBX must be configured with data capability.

Getting there RLC → Configuration Manager → RLC Port Configuration

RLC Port Configuration property sheet

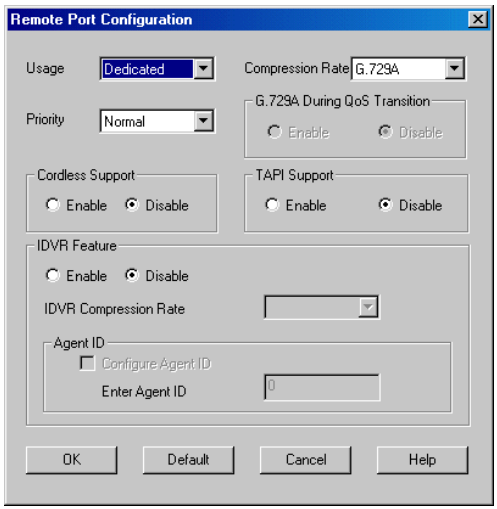


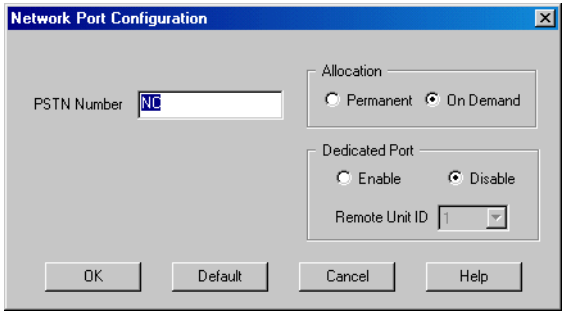
Configuring an RLC port

To configure an RLC port:

1 Click on the appropriate tab for the port you are configuring, as in Ports 0-15 or Ports 16-31 for a 16-port RLC, Ports 0-15, Ports 16-31, Ports 32-47, or Ports 48-63 for a 32-port RLC.

2 In the line for the port you are configuring, choose the type of port you want to configure as follows:

IF you want to configure a	THEN
remote port,	complete the following steps: **a** Click on the **Remote** option button on the line of the port number you are configuring. **b** Click on the **Configure** button on the same line. **Result:** The Remote Port Configuration dialog box displays, similar to the following:  **c** Select the desired settings according to the "Remote Port Configuration field descriptions" on page 190. **d** Click on the **OK** button to save the information to a temporary file on your administration PC.

IF you want to configure a	THEN
network port,	complete the following steps: **a** Click on the **Network Port** option button on the line of the port number you are configuring. **b** Click on the **Configure** button on the same line. **Result:** The Network Port Configuration dialog box displays, similar to the following:  **c** Select the desired settings according to the "Network Port Configuration field descriptions", on page 194. **d** Click on the **OK** button to save the information to a temporary file on your administration PC.

5 Click on the **Send** button to update the RLC with the new information.

Result: The administration PC saves the changes in a temporary file.

6 To save changes to the RLC's Flash memory, select Upload → Save to Flash from the Menu Bar.

Note: Refer to page 168 for information on the Integrated Digital Voice Recorder (IDVR).

Remote Port Configuration field descriptions

Field	Description
Usage	■ Select **Dedicated** to configure this port for use by one DN only. ■ Select **MultiUser** to configure this port for use in a time-share fashion by a variety of remote units or different ports on the same remote unit. ■ Select **Dynamic Pool** to configure this port for use as part of a dynamic pool. Ports in this pool can be dynamically assigned to any remote port that requests access to a port in the RLC port pool.
Compression Rate	■ Select **G.711** to enable transmission at 64 Kbps on this port. ■ Select **G.726** to enable transmission at 32 Kbps on this port. ■ Select **G.729A** to enable transmission at 8 Kbps on this port. ■ Select **G.729A/FAX** to enable transmission at 9.6 Kbps stepped down to 7.2. 4.8, or 2.4 Kbps on this port. **Note:** Ports for facsimile (fax) machines must be configured with G.729A/FAX compression for proper operation.

Field	Description
Priority	■ Select **PSTN Only** to allow access only to the PSTN. PSTN-only ports do not move between networks according to QoS levels. Meridian digital telephone sets that place calls to PSTN-only telephone sets when there is not enough PSTN bandwidth available receive an error message. In this situation, `Bandwidth Limit` displays on the calling digital telephone set. **Note:** Calls can be placed to PSTN-only sets if signaling is over IP but the ISDN is unavailable. Eventually, Remote Office releases the call and displays a `Bandwidth Limit` message. ■ Select **High** to allow access either to the PSTN or the IP network based on QoS. Calls through High priority ports move to the PSTN first in a QoS transition. In recovery situations, when IP QoS returns to within configured limits, calls through High priority ports return to the IP network last, ensuring the most consistent QoS. ■ Select **Normal** to allow access to either the PSTN or the IP network based on QoS. Calls through Normal priority ports move to the PSTN only after all calls through High priority ports make the transition. In recovery situations, as QoS on the IP network returns to within configured limits, calls through Normal priority ports return to the IP network first. ■ Select **IP Only** to allow access only to the IP network. IP-only ports do not move between networks according to QoS levels.

Field	Description
G.729 During QoS Transition	Enabling this setting minimizes the number of PSTN trunks required for QoS transition situations. It is only active when the configured compression rate is G.711 or G.726. ■ Click on the **Enable** option button if you want to allow the RLC and the Remote Office 9150 unit unit to change configured G.711 or G.726 compression algorithms during QoS transitions on this port. ■ Click on the **Disable** option button if you do not want to allow compression algorithm changes during QoS transitions on this port. **Note:** You must disable this option if the system or port is configured as PSTN only. If you do not disable this option, the system does not allow PSTN-only ports to use compression algorithms other than G.729A.
Cordless Support	RLC ports allow you to use either corded telephones or cordless telephones. ■ Click on the **Enable** option button if you want this port to provide service only to cordless telephones, such as M2616CT. ■ Click on the **Disable** option button if you want this port to provide service only to corded telephones, such as M2616. **Note:** Misconfiguration of this field causes incorrect remote telephone operation.

Field	Description
TAPI Support	When you enable Telephone Application Programming Interface (TAPI) support, telephones using the selected port can interact with a TAPI server such as Meridian Communicator. ■ Click on the **Enable** option button if you want this port to interact with a TAPI server. ■ Click on the **Disable** option button if you want to prevent this port from interacting with a TAPI server. When configured for TAPI support, the RLC allocates DSP and bandwidth resources whenever a line key indicator goes active and stays active for Multiple Appearance DNs. To prevent the over-allocation of these resources during midnight routines, either disable LD 35, or configure the RLC as Offline during this period. **Note:** You must configure CS 2100 ATA sets and CS 2100 AAB sets for TAPI support for them to function properly.
IDVR Feature **IDVR Compression Rate**	Refer to page 168 for information on the Integrated Digital Voice Recorder (IDVR).

Network Port Configuration field descriptions

Field	Description
PSTN Number	Enter the port's DN in the PSTN Number field. (This is the DN programmed on the switch that the remote unit uses to contact the RLC.)
Allocation	The allocation setting refers to the connection status of the port being configured. ■ Click on the **Permanent** option button if you want connections established over the port you are configuring to remain up until the remote unit goes offline. ■ Click on the **On Demand** option button if you want connections established over this port to go down when they are no longer needed. Connections over ports configured as On Demand remain up until the minimum call duration timer expires. When using the PSTN, call-establishment takes longer in On Demand mode than in Permanent mode. This is because, in On Demand mode, the Remote Office unit or RLC must establish a new connection for the call. In Permanent mode, the connection already exists.

Field	Description
Dedicated Port	To prevent glare conditions (RLC and Remote Office 9150 unit simultaneously are attempting to dial each other in an effort to establish a communication path) on the existing dedicated network port, you must reserve a secondary network port as an alternate path. Enabling a dedicated port prevents the occurrence of glare by providing separate calling paths for both the RLC and Remote Office 9150 unit. ■ Click on the **Enable** option button if you want this port to be a dedicated network port. ■ Click on the **Disable** option button if you do not want this port to be a dedicated network port. The default is Disable.
Dedicated Port: Remote Unit ID	Select the Unit ID of the Remote Office unit that the dedicated port is to belong to. Valid options are 1 through 20.

IDVR Feature Key Configuration field descriptions

Field	Description
IDVR Status **Key Feature** **Key Number** **IDVR Compression Rate**	Refer to page 168 for information on the Integrated Digital Voice Recorder (IDVR).

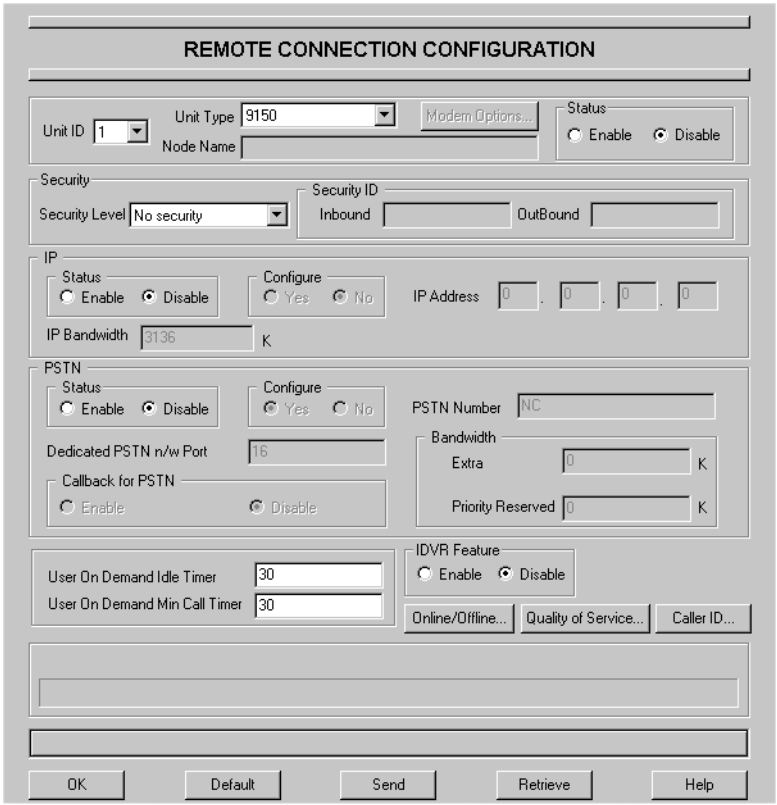
Remote connection configuration

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

- security
- IP connection
- PSTN connection
- call timers

Getting there RLC → Configuration Manager → Remote Connection Configuration

Remote Connection Configuration property sheet



Modem options

This setting helps minimize the time required to establish a modem connection when using a Remote Office 911x series unit with an on-demand allocation over the PSTN. Click on this button to access a dialog box where you configure the length of the answer tone on the answering modem when establishing a connection between an RLC and a Remote Office 911x series unit. The answer tone disables echo cancellers on long distance calls so that modem training is not disrupted.

Note: The answer tone length represents a portion of the total time required for the 911x and RLC to call, train and establish a connection.

V.32 Answer Tone Duration

The RLC passes this setting to the Remote Office 911x series unit when it connects for the first time. For subsequent calls, the Remote Office 911x series unit answers the modem with an answer tone of the correct duration.

Move the slider to the desired length of the answer tone on the receiving modem according to the guidelines in the following table.

Note: This table is only a guide. Your individual situation (exact length of your connections, long distance carrier, and so on) dictates the specific setting that you need to configure. Start with the default setting and test from there. If the connection does not establish, try configuring a longer answer tone by moving the slider farther to the right

Setting	Explanation
Min (Local Calls Only)	Move the slider toward this setting if the RLC and Remote Office 911x series unit are local to one another.
Avg (Long Distance)	This is the default setting. Move the slider closer to this setting for long distance calls within the same country.
Max (Very Long/International)	Move the slider toward this setting if the RLC and Remote Office 911x series unit are very far apart, or in different countries.

Security

The RLC offers three security levels. For an explanation of each of these levels, refer to “Multiple security levels” on page 21.

To configure security for the RLC:

1. Choose the desired security level in the Security Level drop down box on the Remote Connection Configuration property sheet.
2. If you select Provisioned security, you must also enter a 10-digit Outbound Security identifier and a 10-digit Inbound Security identifier. To see how these Security identifiers effect RLC and Remote Office operation, refer to “Multiple security levels” on page 21.

IP connection

To allow a remote unit to establish VoIP connection with the RLC:

1. Enable the VoIP functionality on the IP network for that unit by selecting the option button located in the Status section.
2. Select the Yes option button located in the IP: Configure section.
3. Enter the unit’s IP address in the IP Address fields.
4. Determine the IP Bandwidth using data rate values provided in the Bandwidth usage table located in the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103). Calculate the number of simultaneous calls allowable on your WAN. This depends on the following information:
   - compression algorithms used by the call (refer to the table below)
   - your Wide Area Network (WAN) type
   - whether Voice Activity Detection (VAD) is enabled or disabled

Compression algorithm	Required voice bandwidth in Kbps
G.711	64
G.726	32
G.729A	8
G.729A/FAX	14.4

IP Bandwidth calculation examples (using Peak Data Rate values):

- For a one Mbyte Frame Relay WAN supporting only G.711 calls, enter 848 in the IP Bandwidth field according to the following calculation:

  1024K (1 Mbyte) - 16K for signaling = 1008K of available bandwidth
  1008K/76Kbps (peak data rate for a G.711 call according to the Bandwidth Usage table) = 13
  therefore,
  IP Bandwidth = (13 G.711 calls * 64K [required voice bandwidth from the table above]) + 16K (for signaling) = 832 + 16 = **848K**

- For a one Mbyte Frame Relay WAN supporting only G.729A calls, enter 0 in the IP Bandwidth field according to the following calculation:

  1024 (1 Mbyte) - 16K for signaling = 1008K of available bandwidth
  1008/20Kbps (peak data rate for a G.729A call according to the Bandwidth Usage table) = 50
  therefore,
  IP Bandwidth = (50 G.729A calls * 8K [required voice bandwidth according to the table above]) + 16K (for signaling) = 400 + 16 = **416K**

  Note: Since the maximum number of simultaneous calls possible through a Remote Office system is 32 calls, 50 simultaneous calls are not possible. Therefore, the proper IP Bandwidth setting is 0. Zero (0) is the setting for no bandwidth limit.

- For a 128K Frame Relay WAN supporting up to two G.726 and one G.729A call, enter 88 in the IP Bandwidth field according to the following calculation:

  (2 calls * 44K [peak data rate for a G.726 call according to the Bandwidth Usage table]) + (1 call * 22K [peak data rate for a G.729A call according to the Bandwidth Usage table]) + 16K (for signaling) = 88 + 22 + 16 =126K
  therefore,
  IP Bandwidth = (2 G.726 calls * 32K required voice bandwidth from the table above) + (1 G.729A call * 8K required voice bandwidth from the table above) + 16K (for signaling) = (2 * 32) + (1 * 8) + 16 = 64 + 8 + 16 = **88K**

PSTN configuration

To allow a remote unit to establish PSTN connections with the RLC:

1. Click on the **Enable** option button located in the PSTN: Status section to use the PSTN mode with the remote unit indicated in the Unit ID field.
2. Click on the **Yes** option button located in the PSTN: Configure section to manually configure the PSTN number used by the RLC for initiating a PSTN connection to the remote site.
3. Enter the PSTN number that the RLC must dial to connect to the remote unit in the PSTN Number field.

You must configure PSTN numbers including, the ISDN numbers, in a specific manner. Please read the following examples carefully.

Configuring seven-digit ISDN numbers

If the service documents supplied by the BRI service provider contain a seven-digit ISDN number, then choose from among the following options to configure the number on your Remote Office unit:

- Remote Office 9150 unit BRI configuration

  Configure the PSTN numbers with the seven digits provided by the Central Office without area codes. For example:

  — 5551000 configured against the corresponding B-channel, not 2145551000

- RLC Remote Connection Configuration

  Use the # delimiter to separate the Trunk Access code and area code part of the PSTN number. For example:

  — #9#5551000 (not 95551000) where “5551000” is the primary Remote Office 9150 B-channel

  — #91214#5551000 (if long distance between units), not 92145552000

- RLC Network Port configuration

  Enter the Network Port PSTN Number exactly as the Remote Office unit must dial it. For example:

  — 5552000 (for seven-digit local call) where 5552000 is a PBX DID data port number

  — 12125552000 (if long distance)

— 912125552000 (if long distance and the 9150 BRI CO uses a “9” access code)

Configuring 10-digit ISDN numbers

If the service documents supplied by the BRI service provider contains a 10-digit ISDN number, then the configuration is as follows:

- Remote Office 9150 BRI configuration

  Configure the PSTN numbers with the 10 digits provided. For example: 2145551000 configured on the corresponding B-channel.

- RLC Remote Connection Configuration

  Use the # delimiter to separate the Trunk Access code from the PSTN number. For example:

  — #9#2145551000 (not 92145551000) where “5551000” is the primary Remote Office 9150 unit B-channel and “9” is the Trunk Access Code.

  — #91#2145551000 (if long distance)

- RLC Network Port configuration

  Enter the Network Port PSTN Number exactly as the Remote Office unit must dial it. For example:

  — 5552000 (for seven digit local call) where 5552000 is a PBX DID data port number

  — 12125552000 (if long distance)

  — 912125552000 (if long distance and the Remote Office 9150 BRI CO uses a 9 access code)

Configuring 911x PSTN connections

To configure a PSTN Remote Office 911x series unit:

1. Access the RLC Connection Configuration sheet in Configuration Manager.
2. Enter the DID number of the dedicated PSTN network port on the RLC for the Remote Office 911x series unit in the PSTN Number to Connect to RLC field.
3. Click on the **OK** button.

Special configuration for Callback for PSTN

The Callback for PSTN field on the RLC Remote Connection Configuration property sheet allows you to enable and disable Callback. The default is Callback for PSTN disabled. This means that the RLC places data calls to the Remote Office 9150 unit to establish additional bandwidth during normal operation. If you enable Callback for PSTN, the Remote Office 9150 unit places the call to the RLC to establish additional bandwidth.

Note: During a RLC or Remote Office 9150 reset, or during a sudden IP network failure, both the RLC and the Remote Office 9150 unit attempt to call each other to establish the Primary Signaling Link. When this occurs, either system can actually establish the first connection. Follow the guidelines below when configuring callback for PSTN.

If Callback for PSTN is disabled:

1. Configure the Primary Network Port with a DID number on the host PBX that is routed over a data capable PRI.
2. Configure either DID numbers or internal DNs on all other network ports (one per B Channel).

If Callback for PSTN is enabled:

1. Configure the Primary Network Port with a DID number on the host PBX routed over a data capable PRI.
2. Configure DID numbers on all other network ports (one per B Channel).

Minimum call duration timers and Idle timers

The RLC uses minimum call duration timers and idle timers to help control PSTN costs. For a detailed discussion of these timers, refer to “Timers” on page 25. For information on configuring these timers, refer to “User On Demand Idle Timer” and “User On Demand Min Call Timer” on page 209.

Configuring remote connection settings

To configure remote connection settings:

1. Complete the fields as described in “Remote Connection Configuration field descriptions” on page 205.
2. Click on the **OK** button.

   Result: Configuration Manager writes the changes to a temporary file on the administration PC.
3. Click on the **Send** button to update the RLC with the new information.

   Note: To save changes to the RLC’s Flash memory, select Upload → Save to Flash from the Menu Bar.

Remote Connection Configuration field descriptions

Field	Description
Unit ID	Select the site number assigned to the remote unit you are configuring. Valid options are 1 through 20.
Unit Type	Select 911X, or 9150 according to the Remote Office unit you are configuring at the remote site. **Note:** A maximum of eight Remote Office 9150 units can be connected to the same RLC. The default is 9150.
Node Name	This display only field provides the Node Name of the Remote Office unit. When you enter the Node Name on the 9150 or 911x System Configuration property sheet, this field automatically populates to allow you to identify remote units by name when viewing the Remote Connection Configuration property sheet.
Modem options	Click on the **Modem Options** button if you want to configure the length of the answer tone on the answering modem. **Note:** The answer tone is needed to disable the echo cancellers on long distance calls.
Status	Select whether you want to process calls through this port. ■ Click on the **Enable** option button to activate the remote unit. ■ Click on the **Disable** option button to deactivate the remote unit. The default is Disable.

Field	Description
Security Level	Select the desired security level. Valid options are No Security, Caller ID security, or Provisioned security. The default is No Security.
Security ID: Inbound	If you selected provisioned security, then enter the Security ID, up to 10 digits in length, that must be presented by calls before they are received at this site.
Security ID: Outbound	If you selected provisioned security, then enter the Security ID, up to 10 digits in length, that must be presented by calls before they are allowed to go out from this site.
IP: Status	Select whether or not VoIP is the primary connection type to the remote office. ■ Click on the **Enable** option button to choose the IP network as the primary connection type to the remote unit. ■ Click on the **Disable** option button to disable connectivity to the remote unit over the IP network. The default is Disable.

Field	Description
IP: Configure	Select whether you want to allow the RLC to initiate IP connections to the remote site. ■ Click on the **Yes** option button to configure a static IP address for the remote unit. **Note:** The RLC uses this address for connections to the remote unit. ■ Click on the **No** option button if you do not wish to configure an IP address for the remote unit. **Note:** If you select Yes, you must also configure an IP address for the remote unit. The default is No.
IP Address	Enter the remote unit's IP address if you want to be able to initiate IP connections to the remote site from the RLC.
IP Bandwidth	Enter the total amount of voice bandwidth needed for the maximum number of simultaneously active telephone calls over your WAN. When the configured IP Bandwidth limit is reached, PSTN bandwidth is established. If PSTN is disabled, then a Bandwidth Limit error message displays to the user of the Remote Office 9150 unit. This feature does not apply to Remote Office 911x series or Meridian Digital Telephone IP Adapter units. The default is 3136K.
PSTN: Status	Select whether you want to use the PSTN mode with this remote unit. ■ Click on the **Enable** option button to allow the RLC to connect to the remote unit over the PSTN. ■ Click on the **Disable** option button to prevent the RLC from connecting to the remote unit over the PSTN. The default is Disable.

Field	Description
PSTN: Configure	Select whether you want to manually configure the PSTN number used by the RLC for initiating a PSTN connection to the remote site. ■ Click on the **Yes** option button to manually configure the PSTN number. ■ Click on the **No** option button if you do not wish to manually configure the PSTN number. **Note:** If you select Yes, you must also configure a PSTN number for the remote unit. The default is Yes.
PSTN Number	Enter the PSTN number the RLC must dial to connect to the remote unit. The default is NC (Not Configured). For configuration details, refer to “PSTN configuration” on page 201.
Dedicated PSTN n/w (network) Port	Enter the RLC network port number that is dedicated to support the remote unit. The default is 16. **Note:** All network ports that are not dedicated are used as a pool to support additional network connections to remote units.
Bandwidth: Extra	Enter the minimum number of Kbytes of bandwidth to have available at any time for PSTN access to the remote unit. The default is 0.
Bandwidth: Priority Reserved	Enter the Kbytes of PSTN bandwidth you would like to reserve for high priority DNs. The default is 0.

Field	Description
Callback for PSTN	The Callback for PSTN setting determines the site that initiates additional trunk connections when the RLC identifies the need for additional bandwidth. ■ Click on the **Enable** option button if you want the PBX to initiate the additional trunk connections. ■ Click on the **Disable** option button if you want the RLC to initiate the additional connections. The default is Disable.
User On Demand Idle Timer	Enter the maximum number of seconds that a PSTN connection can remain idle at this remote site before the RLC closes it. For more details, refer to "Minimum call duration timers and Idle timers" on page 203. The default is 30.
User On Demand Min Call Timer	Enter the minimum number of seconds that a PSTN connection must remain open at this remote site before the RLC closes it. For more details, refer to "Minimum call duration timers and Idle timers" on page 203. The default is 30.
IDVR Feature	Refer to page 168 for information on the Integrated Digital Voice Recorder (IDVR).
Online/Offline	Click on the **Online/Offline** button to edit the online/offline table for the remote site. Refer to "Online/Offline table configuration" on page 219 for details on configuring this table.
Quality of Service	Click on the **Quality of Service** button to edit the Quality of Service (QoS) Transitioning Technology settings for the remote site. Refer to "Configuring QoS" on page 211 for information on configuring these settings.

Field	Description
Caller ID	If you have chosen caller ID security for this remote site, click on the **Caller ID** button to enter the telephone numbers that you want to have access to this remote site.

Configuring QoS

This section shows you how to configure the RLC with quality and duration values for Nortel Networks' patented QoS Transitioning Technology.

QoS Transitioning Technology allows you to define *acceptable* voice QoS for Remote Office telephone calls routed using Voice over Internet Protocol (VoIP). The Signal Degrade slide control allows you to set the point where poor voice QoS causes the RLC to transition calls to the PSTN for better QoS. The Signal Recover slide control identifies the IP voice QoS level where you want the RLC to recover calls to the IP network.

You can also define the following duration parameters:

- The degrade duration is the time (in seconds) that QoS must remain below the degrade threshold before the RLC transitions calls to the PSTN.
- The recover duration is the time (in minutes) that QoS must remain above the recover threshold before the RLC recovers the call to the IP network.

The units of the acceptable duration for recovery are minutes rather than seconds in an attempt to minimize *transition thrashing.* Transition thrashing is the rapid transition and recovery between networks. This can occur when QoS hovers around configured degrade and recover thresholds. This phenomenon produces higher than normal PSTN charges.

Note: QoS problems can sometimes be addressed through prioritization of voice packets. For more information, refer to "QoS on shared networks" on page 19.

QoS transition recovery

Due to the requirement for on-demand router support, the IP network is not continually tested during QoS transition situations. It is tested only when there are active voice calls over the PSTN. As a result, transitioning needs active calls for the user-configured recovery period in order to switch back to the IP network.

If you test QoS transition by disconnecting the Ethernet cable from the Meridian unit, or RLC, expect up to a 20-second delay before the Meridian unit can place or receive a call. You do not encounter this delay when the network degrades and calls switch to BRI as designed.

If a QoS transition occurs while a Remote Office unit is sending or receiving a fax, the packets lost prior to the transition can result in:

- a fax that is not readable at the receiving end
- error messages that appear on both the sending and receiving fax machines

If this occurs, send the fax again.

More information

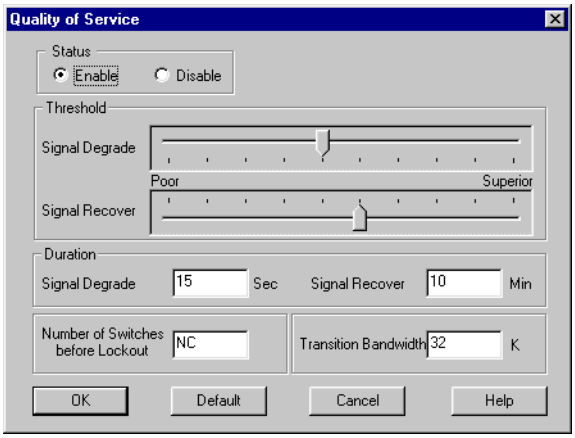
Refer to the *Remote Office Network Engineering Guidelines* (NTP 555-8421-103) for detailed information describing QoS Transitioning Technology. To locate this document, click on the **Technical Documentation** link at the following website:

www.nortelnetworks.com

Getting there

RLC → Configuration Manager → Remote Connection Configuration → Quality of Service

Quality of Service dialog box



Configuring QoS

The slide controls allow 10 settings ranging from poor to superior, within the following boundaries:

- 1 (poor) equates to a MOS (Mean Opinion Score) value of 3.0, as calculated by the RLC and based upon the ITU E-Model for serviceability and service integrity performance
- 10 (superior) equates to a MOS value of 4.0

Since the ITU E-Model uses network delay as its sole point of reference, the RLC also factors in average packet-loss to obtain the MOS value. For example, if the user sets the threshold to a MOS value of 3.5 (center tick of slide control), the following scenario can occur. The measured delay on the network may indeed be less than a score of 3.5 according to the ITU E-model. However, excessive packet loss can lower the MOS value calculated by the RLC. In this scenario, the RLC moves the call from the IP network to the PSTN. This move ensures an acceptable QoS for the user, based on real network conditions.

QoS configuration procedure

1 Complete the fields as described in “Quality of Service field descriptions” on page 214.

2 Click on the **OK** button.

Result: Configuration Manager writes the changes to a temporary file on the administration PC.

3 Click on the **Send** button to update the RLC with the new information.

Note: To save changes to the RLC’s Flash memory, select Upload → Save to Flash from the Menu Bar.

Quality of Service field descriptions

Field	Description
Status	■ Click on the **Enable** option button to allow QoS transitions to occur when the QoS on the IP network degrades. ■ Click on the **Disable** option button if you do not want to use the QoS Transitioning Technology. The default is Enable.
Threshold: Signal Degrade	Move the indicator to the appropriate point on the sliding scale, a relative value between poor and superior.
Threshold: Signal Recover	Move the indicator to the appropriate point on the sliding scale, a relative value between poor and superior.
Duration: Signal Degrade	Enter a value, in seconds, between 1 and 60. If poor voice quality lasts for the specified duration, then calls are moved from the IP network to the PSTN. The default is 15 seconds.
Duration: Signal Recover	Enter a value, in minutes, between 1 and 10. When the improved voice quality lasts for the duration value chosen (in minutes), then calls are moved back to the IP network. The default is 10 minutes.
Number of Switches before Lockout	Enter the number of transitions between the IP network and PSTN in any 24-hour period that causes the RLC to stop making the transition. The default is NC (Not Configured).

Field	Description
Transition Bandwidth	Enter the amount of bandwidth in Kbytes that you want the RLC to have available at all times for use when transitioning between the IP network and PSTN. The default is 32 K.

How the online/offline table works

Use the online/offline table to schedule the times that the RLC makes a PSTN connection available to an RLC port. The online/offline table gives you the ability to ensure that potentially costly PSTN/ISDN or long distance connections do not stay up after business hours. If the offline command occurs while the connection is in use, Remote Office system users at the remote site can override table settings.

Notes:

- When a remote unit is in the offline mode, users cannot place host-controlled calls with that unit.
- Users can override the online/offline table to establish or terminate a connection to the network.

Online/offline configuration example

The online/offline table allows you to make up to eight entries per day, every day of the week, for each remote site. The following is an example of a standard online/offline program for an RLC port.

Entry	State	State
Entry 1	At 8:00 a.m., the RLC establishes the remote site's PSTN connection.	Online
Entry 2	At 11:30 a.m., (a common lunchtime) the RLC disables the PSTN connection.	Offline
Entry 3	At 12:30 p.m., (the end of lunchtime) the RLC re-enables the PSTN connection.	Online
Entry 4	And at 5:00 p.m., the RLC disables the PSTN connection for the day.	Offline

Online/Offline table overrides

Any remote user can override the settings of the online/offline table if the table attempts to terminate the connection during a call. A buzz alerts users at the remote site that the connection is going down in 30 seconds. After the initial warning, users can enter the online SPRE code on their telephone key pads to override the termination of the connection. The warning buzz repeats itself 20 and 10 seconds before the system terminates the connection. Any user at the remote site can avoid going offline by entering the online SPRE code.

Multiple offline periods

You can configure multiple offline entries into the table without configuring online entries between each offline entries. In this way, you can program the RLC to terminate a connection that has been left open if a remote site user is forced to override a scheduled PSTN termination.

For example, Mr. Smith, a remote site user, begins a business call with Mr. Jones, at 4:45 p.m. on a Friday. The RLC is programmed to terminate his PSTN connection at 5:00 p.m. However, Mr. Smith overrides the scheduled termination, and the call continues for another 45 minutes. The business call succeeds, but the expensive PSTN connection remains up. If the usual schedule were followed, the connection would not be terminated until lunch time on the following Monday.

Fortunately, Mr. Smith's system administrator foresaw this situation and configured offline commands for 6:00, 7:00, and 8:00 p.m. So, the RLC terminates the PSTN connection at 6:00 p.m. Mr. Smith's company accrues only 15 minutes of unnecessary PSTN charges.

How the remote site goes online

When going offline, the remote unit's offline timer activates. When the timer expires, the remote unit automatically initiates a "going online" request to the host PBX. If the RLC receives the request successfully, the remote site and its associated digital telephones go online.

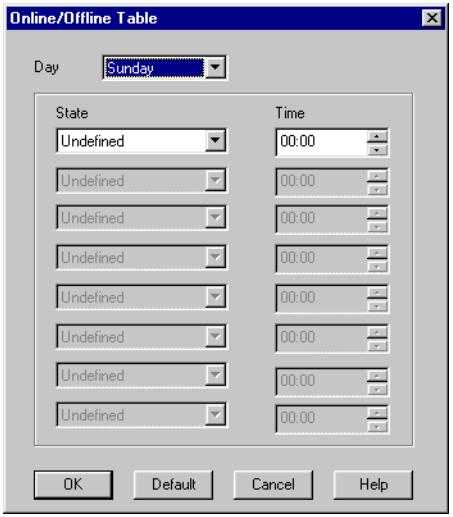
If you configure no online entries in the online/offline table, the RLC instructs the remote unit to go offline forever each time it processes an offline entry. To go back online, a remote user must enter the online SPRE code in order to place host-controlled calls on either the PSTN or IP network.

Online/Offline table configuration

The Online/Offline Table allows you to enter up to eight entries per day for each remote site, every day of the week. You can define each entry as Online, Offline, or Undefined.

Getting there RLC → Configuration Manager → Remote Connection Configuration → Online/Offline Table

Online/Offline Table



Configuring an Online/Offline Table

To configure the Online/Offline Table:

1. Access the Remote Connection Configuration property sheet.
2. Ensure that the Unit ID drop down box shows the Unit ID for the remote unit you want to configure an Online/Offline Table for. If it does not, choose the proper Unit ID from the drop down box, such as **1—20**.
3. Ensure that the Unit Type drop down box properly reflects the remote unit you want to configure an Online/Offline Table for. If it does not, choose the proper Unit Type from the drop down box, such as **9150** or **911X**.
4. Click on the **Online/Offline** button.

   Result: The Online/Offline Table dialog box displays. (Refer to “Online/ Offline Table” on page 219.)
5. From the Day drop down box, select the day of the week that you want the remote unit to have access to the network (PSTN or IP).
6. In the enabled State drop down box, choose **Online** or **Offline**, according to the command you want the system to initiate for this remote site.

   Result: Configuration Manager enables the associated Time list box and the State and Time list boxes immediately below. The chosen state (**Online** or **Offline**) displays in the list box described in step 6.

   Note: If you choose **Undefined**, the subsequent list boxes remain disabled. Configuration Manager takes your choice of **Undefined** to be an indication that you do not want to configure more commands in this Online/Offline Table.
7. In the associated Time list box, choose the time (24-hour time format) that you would like Configuration Manager to initiate the state chosen in step 5.
8. As you make selections in the State drop down box, Configuration Manager enables list boxes in the subsequent line, with the opposite selection.

chosen as a default selection. For example, **Offline** (if you chose **Online** in step 6) or **Online** (if you chose **Offline** in step 6).

Note: You can make your desired Online/Offline Table selection in any enabled field in any order.

IF you want to	THEN
continue configuring entries (up to eight) in the Online/Offline Table for this remote unit,	return to step 6.
stop configuring the Online/Offline Table for this remote unit,	click on the **OK** button.

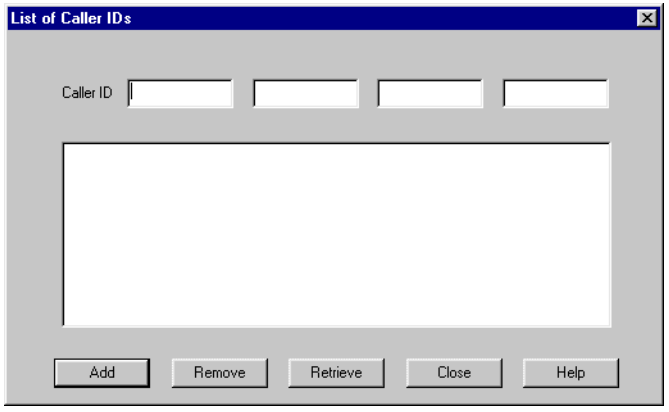
Caller ID configuration

Note: This procedure applies to Remote Office 9150 units only.

In the list of Caller IDs dialog box, enter the DNs of every B-channel assigned to the remote unit you are configuring. The Unit ID field of the associated Remote Connection Configuration property sheet identifies the remote site these Caller IDs apply to. Enter up to 20 telephone numbers using the same format used by the PSTN for presenting these DNs, such as 10 digits or four digits. If you want to use level 2 (Caller ID) security, you must enter the DNs of all associated B-channels. For more information on Caller ID security, refer to "Level 2, caller ID security" on page 21. For the proper procedure to use in Caller ID configuration, refer to "Configuring Caller ID information" on page 223.

Getting there RLC → Configuration Manager → Remote Connection Configuration → Caller ID

List of Caller IDs



Configuring Caller ID information

To configure Caller ID information for a Remote Office 9150 unit:

1. Access the Remote Connection Configuration property sheet. (Refer to “Remote connection configuration” on page 197 for help in locating this property sheet.)
2. Choose the Unit ID of the Remote Office 9150 unit that you want to configure Caller IDs in the Unit ID drop down box, such as **1**–**20**.

   Result: 9150 displays in the Unit Type drop down box. If 9150 does not display in the Unit Type drop down box—if you are completing an offline configuration, for instance—select 9150 from the available options.
3. Click on the **Caller ID** button.

   Result: The Caller ID configuration sheet displays. (Refer to “List of Caller IDs” on page 222.)
4. Enter the telephone numbers of the people to whom you want to grant access to the remote unit in the Caller ID fields.

   Note: Enter up to four Caller IDs.
5. Click on the **Add** button.

   Result: The numbers you entered in the fields display in the larger window below.
6. When you have entered all of the Caller IDs for the ISDN BRI B-channels assigned to this Remote Office 9150 unit, you can configure up to 8, click on the **Close** button.

   Result: Configuration Manager displays the Remote Connection Configuration property sheet.
7. Click on the **OK** button.

   Result: Configuration Manager writes the changes to a temporary file on the administration PC.
8. Click on the **Send** button to update the RLC with the new information.

   Note: To save changes to the RLC’s Flash memory, select Upload → Save to Flash from the Menu Bar.

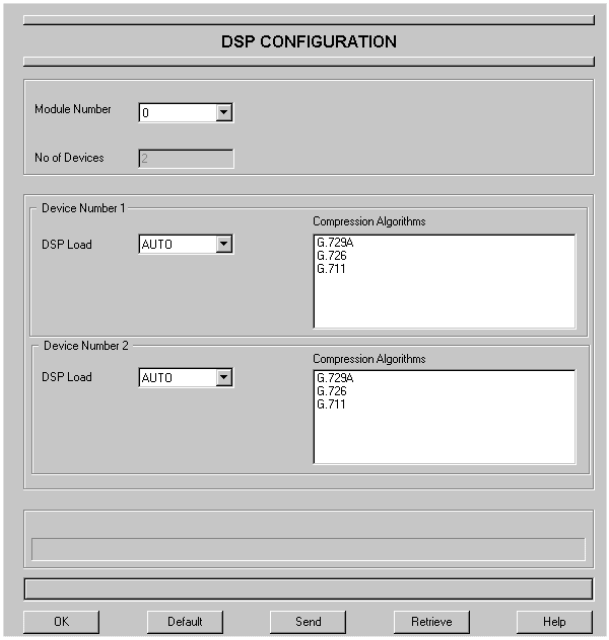
DSP configuration

This section shows you how to configure DSP resources on your RLC. The RLC must provide the same number of voice DSP channels as the maximum number of simultaneous calls your remote services network supports. Each DSP *module* holds two DSP *devices.* Currently, each DSP *device* holds four DSP *channels.* To add eight DSP *channels* to your Remote Office system's voice processing capability, add one DSP application *module.*

Calls made from Remote Office 911x series units require two DSP channels (one voice channel, one modem channel) when operating in PSTN mode. This includes QoS transitions. If you want to configure Remote Office 911x series units for analog modem calls, you must set the RLC DSPs to Remote Office 911x. Each DSP configured for the Remote Office 911x series unit supports four modem only connections (no support for G.711, G.729A, or G.726).

Getting there RLC → Configuration Manager → DSP Configuration

DSP Configuration property sheet



Module identification

The upper portion of the DSP configuration property sheet displays fields that identify the module you are currently configuring. In the Module Number drop down box, choose the module position on the RLC that the DSP module occupies. Module 0 represents the built-in DSP resources on the RLC–the equivalent of one DSP application module.

Device configuration

The middle portion of the property sheet displays information describing the DSP loads, and corresponding compression algorithms that you can select for each DSP device. Remote Office configures the same DSP load to all four channels on the same device. The number of DSP devices on an RLC determines the number of DSP loads that the RLC can accommodate.

Configuring DSPs

To configure DSP modules on your RLC, complete the following steps:

1. Access the DSP Configuration property sheet.
2. Complete the fields as described in “DSP Configuration field descriptions” on page 226.
3. Click on the **OK** button.

   Result: Configuration Manager writes the changes to a temporary file on the administration PC.
4. Click on the **Send** button to update the RLC with the new information.

   Note: To save changes to the RLC’s Flash memory, select Upload → Save to Flash from the Menu Bar.

DSP Configuration field descriptions

Field	Description
Module Number	Select the number of the module that the DSP devices that you want to choose compression algorithms for are located on. **Note:** Module 0 represents the main board (RLC or Remote Office 9150 unit). Modules 1 and higher represent plug-in modules. The default is 0.
No of Devices	This read-only window displays the number of DSP devices available on the DSP module you selected in the Module Number field. Refer to "DSP configuration" on page 224 for an explanation of DSP *devices* versus DSP *modules* and DSP *channels.* This read-only value is 2.
Device Number 1 or 2	
DSP Load **Note:** This description applies to both appearances of this field.	Select the DSP Load providing the collection of compression algorithms that you would like loaded on the selected DSP according to the compression algorithms displayed in the Compression Algorithms window. Valid options are G.729A, 911X, G.723_CONF, and AUTO. The default is AUTO. **Notes:** **1.** G.723_CONF allows you to record telephone calls using IDVR. For more information regarding IDVR, contact your TelStrat representative. **2.** Selecting **AUTO** instructs the RLC to choose a default DSP load. This default load is G.729A, depending on DSP channel availability.

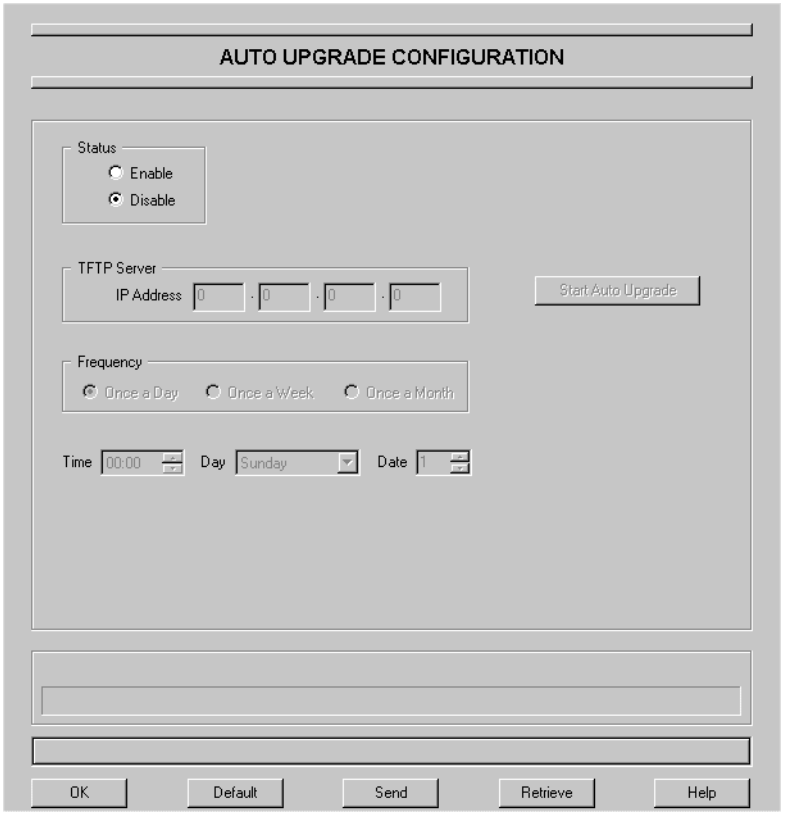
Field	Description
Compression Algorithms **Note:** This description applies to both appearances of this field.	This read-only window displays the combination of compression algorithms that are available in the DSP load selected in the DSP Load drop down list. The compression algorithm (G.711, G.726, or G.729A) used on calls to or from the Remote Office unit stations is dictated by the compression setting configured for the remote port that the call is processed over.

Auto upgrade configuration

Use the Auto Upgrade Configuration property sheet to automatically or on a scheduled basis query a predefined TFTP server and upgrade the firmware for Remote Office units.

Getting there RLC → Configuration Manager → Auto Upgrade Configuration

Auto Upgrade Configuration property sheet



Configuring automatic upgrade

To configure automatic upgrade of your RLC, complete the following steps:

1. Access the Auto Upgrade Configuration property sheet.
2. Complete the fields as described in “Auto Upgrade Configuration field descriptions” on page 230.
3. Click on the **OK** button.

   Result: Configuration Manager writes the changes to a temporary file on the administration PC.
4. Click on the **Send** button to update the RLC with the new information.

   Note: To save changes to the RLC’s Flash memory, select Upload → Save to Flash from the Menu Bar.

Auto Upgrade Configuration field descriptions

Field	Description
Status	■ Click on the **Enable** option button if you want to automatically or on a scheduled basis query a predefined TFTP server and upgrade the firmware for Remote Office units. ■ Click on the **Disable** option button if you do not want to automatically or on a scheduled basis upgrade the firmware for Remote Office units. The default is Disable.
TFTP Server: IP Address	Enter the IP address of the TFTP server you want to query for the upgrade.
Start Auto Upgrade	Click on the **Start Auto Upgrade** button to force the auto upgrade process to begin regardless of the mode and time configuration in the auto upgrade configuration. **Note:** Use caution when forcing the auto upgrade process as the system performs a self-reset on all units to make the new firmware active once the download of new firmware is complete.
Frequency	Click on the option button that identifies how often you want the unit to perform the auto upgrade process: ■ Once a Day ■ Once a Week ■ Once a Month
Time	Select the time of day that you want the unit to perform the auto upgrade process.
Day	Select the day when you want the auto upgrade process to be performed (if you selected "Once a Week" in the Frequency field).

Field	Description
Date	Select the date when you want the auto upgrade process to be performed (if you selected "Once a Month" in the Frequency field).

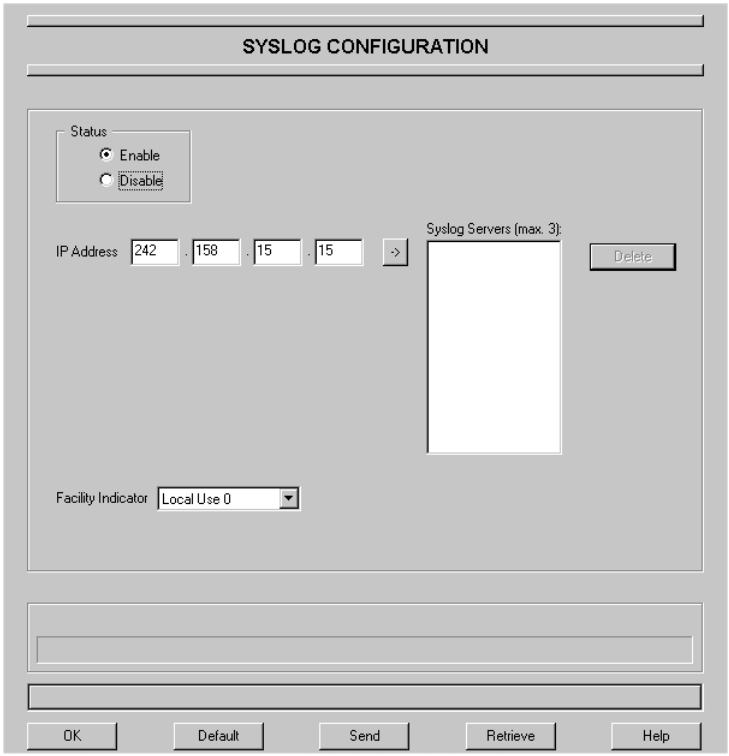
Syslog configuration

Use the Syslog Configuration property sheet to enable syslog functionality and configure up to three syslog server IP addresses for logging all events (display logs) to the syslog server(s) you configure.This feature allows event logs (display logs) to be retained if you reboot or restart the Remote Office unit. Remote Office supports the following syslog collector software:

- Kiwi Syslog Daemon - www.kiwisyslog.com
- WinSyslog - www.winsyslog.com
- tftp32d server - http://tftpd32.jounin.net

Getting there RLC → Configuration Manager → Syslog Configuration

Syslog Configuration property sheet



Configuring syslog functionality

To configure syslog functionality on your RLC, complete the following steps:

1. Access the Syslog Configuration property sheet.
2. Complete the fields as described in “Syslog Configuration field descriptions” on page 234.
3. Click on the **OK** button.

   Result: Configuration Manager writes the changes to a temporary file on the administration PC.
4. Click on the **Send** button to update the RLC with the new information.

   Note: To save changes to the RLC’s Flash memory, select Upload → Save to Flash from the Menu Bar.

Syslog Configuration field descriptions

Field	Description
Status	■ Click on the **Enable** option button if you want to enable the syslog functionality. ■ Click on the **Disable** option button if you do not want to enable the syslog functionality. The default is Disable.
IP Address	Enter the IP Address of the syslog server. Then, press the Enter key or click on the **->** button to add the IP address to the Syslog Servers window. You can enter up to three syslog server IP addresses. **Result:** The IP address of the syslog server displays in the Syslog Servers window.
Delete	To delete a syslog server IP address from the Syslog Servers window, click on the specific IP address that you want to delete and then click on the **Delete** button.
Facility Indicator	Select the facility indicator from the drop down box. Valid options are Local Use 0 through 7.

Chapter 7

Administration

In this chapter

Changing the administration password

Two layers of password security protect the RLC's configuration. To secure the RLC's configuration so that only those with passwords unique to your RLC can make configuration changes, alter the following items:

- Configuration Manager password

  This password prevents unauthorized users from performing offline configuration changes.

- RLC's password

  This password prevents unauthorized users from performing online changes of the configuration residing in the RLC's Flash memory.

Note: Nortel Networks recommends that you change these passwords for logging on to both Configuration Manager and the RLC. Make sure that you record the password and store it in a safe, secure location. If you forget or lose the password, contact your Nortel Networks customer support representative.

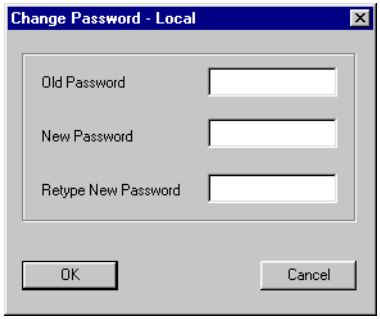
Getting there RLC → Configuration Manager

Changing the Configuration Manager password

To change the Configuration Manager (local) password:

1 From the Menu Bar, choose Connect → Change Password →Local.

Result: The Change Password dialog box displays, similar to the following:



2 Complete the fields in the Change Password dialog box.

3 Click on the **OK** button.

Result: The Password changed successfully dialog box displays.

4 Click on the **OK** button.

Changing the RLC password

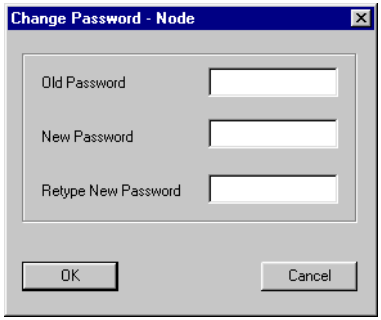
To change the RLC (node) password:

ATTENTION

Do not change the RLC's password until the system is up and working.

1 From the Menu Bar, choose Connect → Change Password → Node.

Result: The Change Password dialog box displays, similar to the following:



2 Complete the fields in the Change Password dialog box.

3 Click on the **OK** button.

Result: The Board Password Changed Successfully dialog box displays.

Note: This means that Configuration Manager has written the password to the RLC's Flash memory.

4 Click on the **OK** button.

5 From the Menu Bar, choose Upload/Download → Save to Flash.

Result: Configuration Manager updates RLC's memory with the new password.

6 Restart the RLC.

Creating a backup configuration file

Create a backup copy of the RLC's configuration by downloading the configuration from Flash memory to a text file on your administration PC. 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 RLC is an extension of the telecommunications and data network. It is extremely important that you keep a backup copy of the RLC's configuration. If the RLC's Flash memory or configuration becomes corrupted or is lost, you can easily restore it.

Store the configuration file in a safe, secure location, such as on backup tape or other media that is stored offsite.

Nortel Networks recommends that you keep the backup files indefinitely.

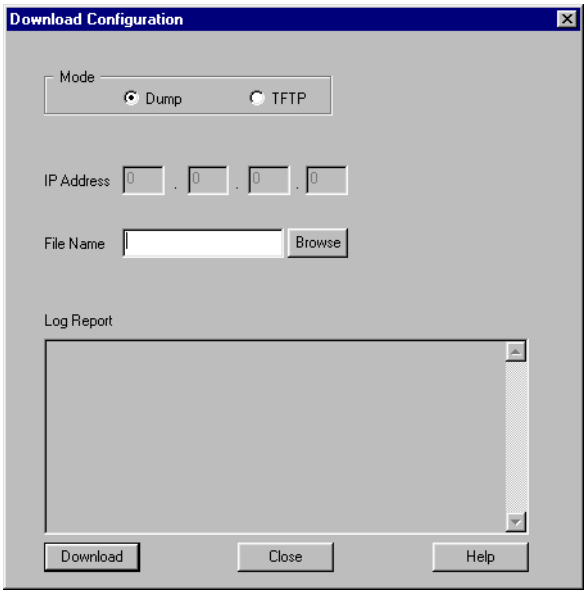
Getting there RLC → Configuration Manager

Creating the backup file

To create the backup file:

1 From the Menu Bar, choose Upload/Download → Download Configuration.

Result: The Download Configuration dialog box displays, similar to the following:



2 Choose the mode you want to use for the file transfer according to the following table:

IF you wish to save the configuration file to	THEN do the following:
the administration PC,	Click on the **Dump** option button.
a different location on the IP network,	1 Click on the **TFTP** option button. **Result:** This enables the IP Address fields. 2 Enter the IP address of the PC that you want to save the configuration file on.

3 Click on the **Browse** button and navigate to the folder where you want to keep the configuration text file.

4 Enter a name for the file in the File name field.

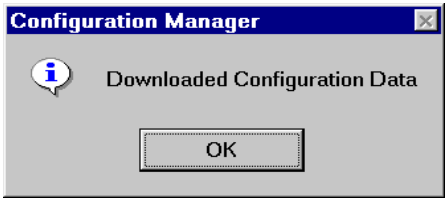
Note: This configuration file becomes your backup file, so ensure the file name is meaningful. The file name's extension must be .TXT.

5 Click on the **Download** button.

Result: The Download configuration dialog box closes, and the following message displays in the status bar at the bottom of the screen:

```
Downloading Config From Board
```

When the download is complete, the Downloaded Configuration Data dialog box displays, similar to the following:



6 Click on the **OK** button.

Note: Flash downloads to remote M39xx telephones can take twice as long compared to when these telephones are connected directly to a standard Nortel digital line card (XDLC).

Restoring the configuration

Restore the configuration to the RLC's Flash memory by uploading a configuration text file from a PC on the same network as the RLC. To do this, perform the upload over the IP network using the TFTP protocol.

Before you begin

Before you can upload the configuration file to the RLC, you must complete the following steps:

1. Start the TFTP server application.
2. Ensure that the TFTP base directory points to the location of the configuration file.

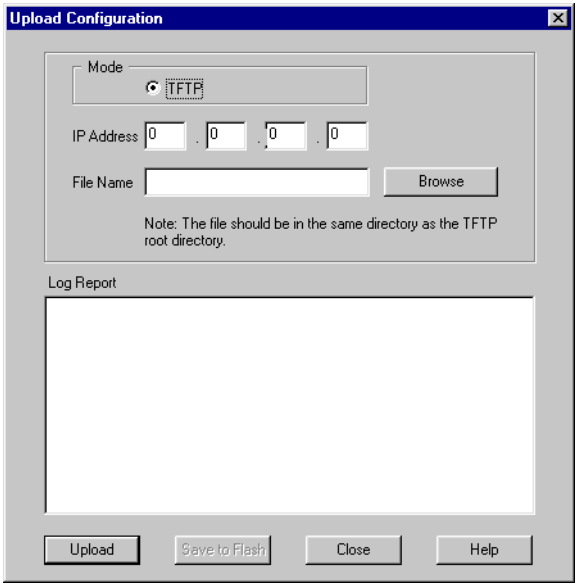
Getting there RLC → Configuration Manager

Uploading a configuration file over the IP network

To upload a configuration file over the IP network:

1 From the Menu Bar, choose → Upload/Download → Upload Configuration.

Result: The Upload Configuration dialog box displays, similar to the following:

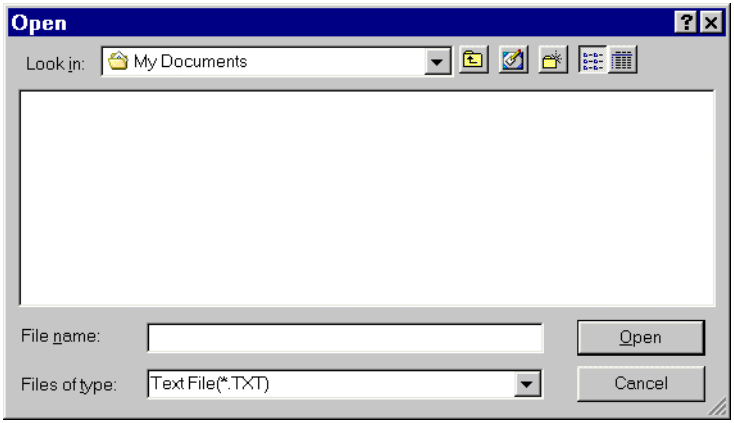


2 Enter the IP address of the TFTP server in the IP Address fields.

Note: Since the TFTP server application is running on your administration PC, this is the IP address of the administration PC.

3 Click on the **Browse** button.

Result: The Open dialog box displays, similar to the following:



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

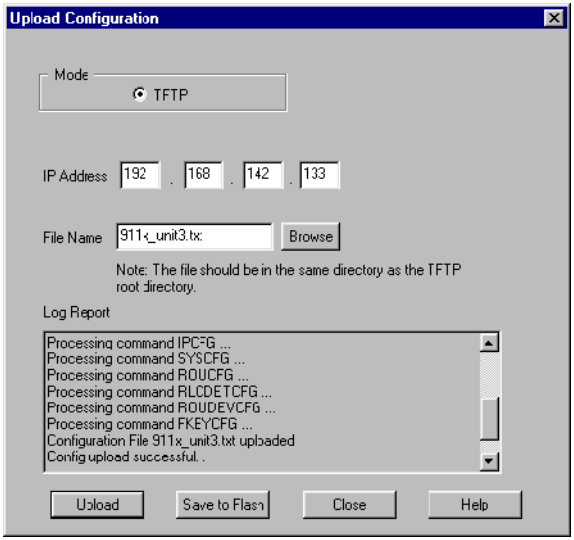
5 Navigate to the folder containing the configuration file.

6 Select the configuration file, and then click on the **Open** button.

Result: The Upload Configuration dialog box displays with the file you selected shown in the File Name field.

7 Click on the **Upload** button.

The middle of the Upload Configuration dialog box displays status messages relating to the upload. 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 RLC's database.

If the configuration upload is interrupted, repeat this procedure immediately.

IF the upload	THEN
is successful,	the following message displays: `CONFIG UPLOAD SUCCESSFUL... USE SAVECFG TO UPDATE FLASH.` Proceed to step 8.
fails,	the following message displays in the middle of the Upload Configuration dialog box: `CONFIG UPLOAD FAILED` For further instructions, refer to Chapter 8, “Troubleshooting”.

8 On the Upload Configuration dialog box, click on the **Save to Flash** button.

Result: The FLASH CONFIG dialog box displays, similar to the following:

9 Click on the **Yes** button.

Result: The following message displays in the status bar at the bottom of the screen:

`Saving to Flash in Progress`

When the save is finished, the following message displays in the middle of the Upload Configuration dialog box:

`CONFIGURATION IS UPDATED INTO FLASH...`

10 Click on the **Close** button.

11 Restart the RLC.

Note: For instructions, refer to “Performing a system restart or shutdown” on page 161.

Display logs

The RLC keeps track of system performance through the maintenance of display logs. Each line, or display log, represents a separate action completed by the unit. Refer to Configuration Manager online Help for a complete listing of all display logs and the condition indicated by each.

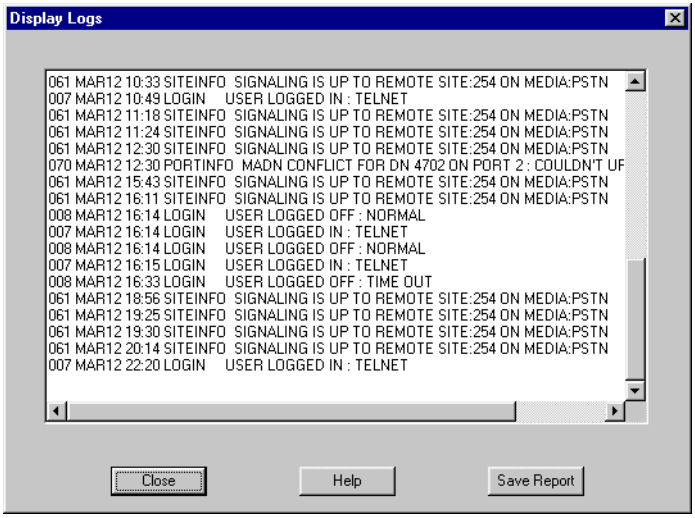
Use the display logs when troubleshooting system problems. Click on the **Save Report** button to print the display logs to a text file, or you can copy the information from the Display Logs window, and paste it into a text file.

Getting there RLC → Configuration Manager

Viewing display logs

From the Menu Bar, choose Alarms/Stats/Logs → Display Logs.

Result: You can view the RLC's display logs in a window similar to the following. You can use the scroll bar to browse through the logs.

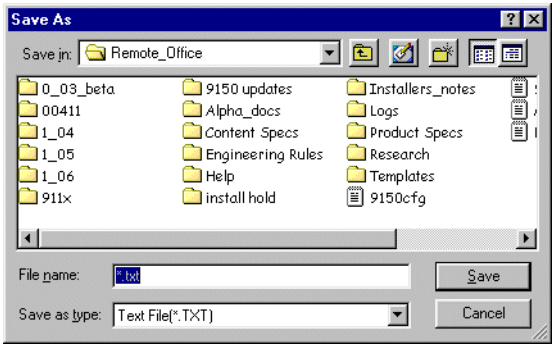


Printing the display logs to a file

If you request technical support, your support representative can ask you to provide a copy of the logs. To recreate the log in a file on your administration PC, follow this procedure:

1 After displaying the logs using the procedure explained under “Viewing display logs” on page 246, click on the **Save Report** button on the Display Logs window.

Result: The Save As dialog box displays, similar to the following:



2 Navigate to the folder where you want to store the log file.

3 Enter a name for the configuration in the File name field.

4 Click on the **Save** button.

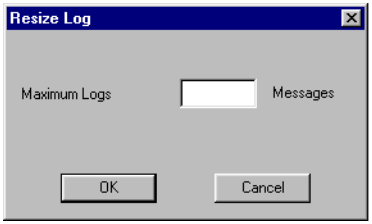
Result: Configuration Manager saves the logs to a text file in the location indicated in the Save As dialog box.

Changing the size of RLC logs

The RLC retains a maximum of 1000 display logs, each requiring one line of text. When the RLC's display logs reach 1000 lines, new display logs overwrite existing display logs on a first in, first out basis. If you want to change the number of display logs retained by the RLC:

1 From the Menu Bar, choose Alarms/Stats/Logs → Resize Logs.

Result: The Resize Log dialog box displays, similar to the following:



Note: "Maximum logs" refers to the number of text lines maintained in the RLC system log. The log holds a maximum of 1000 text lines, or the 1000 most recent display logs, when it shipped from the factory.

2 Enter the maximum number of display logs you want the RLC to keep in the Maximum Logs field.

3 Click on the **OK** button.

Clearing logs

The RLC allows you to delete unneeded information by clearing the display logs that the RLC keeps. To discard or clear display logs that are no longer useful:

1 From the Menu Bar, choose the Alarms/Stats/Logs → Clear Logs.

Result: The CLEAR LOGS dialog box displays, similar to the following:

IF you select	THEN
No,	the Clear logs dialog box closes and the logs remain as they are.
Yes,	■ the RLC deletes its stored display logs. ■ the LOGS cleared dialog box displays, similar to the following:  Click on the **OK** button.

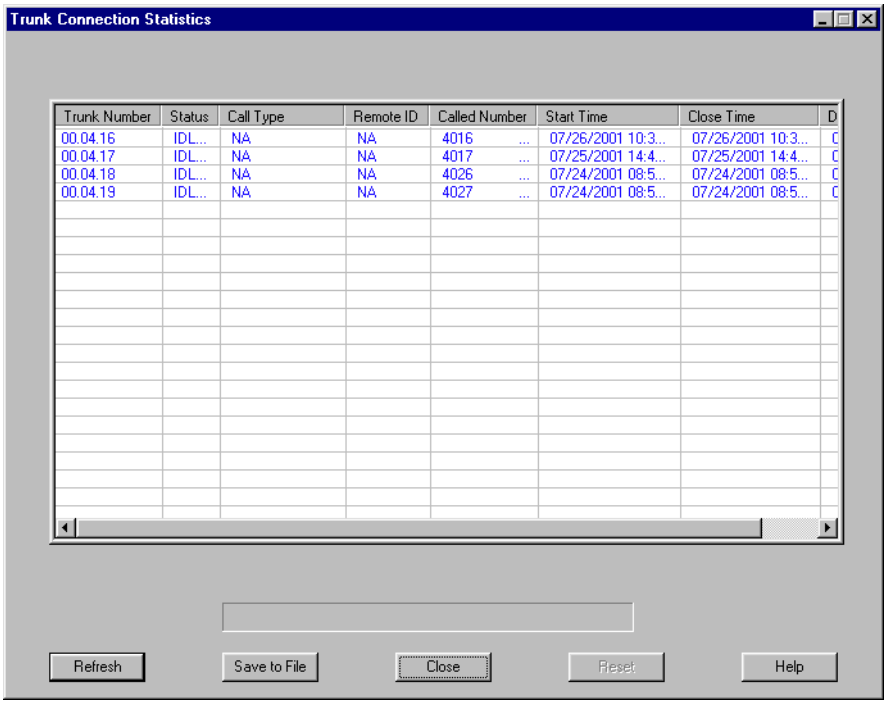
Statistics screens

All statistics screens provided by the Alarms/Stats/Logs menu, function primarily to help you obtain information to provide to technical support personnel, upon request.

Getting there RLC → Configuration Manager

Trunk Connection Statistics

Trunk Connection Statistics show you the PSTN trunk usage for the selected remote site, similar to the following:



To display the Trunk Connection Statistics screen, refer to "Displaying the Trunk Connection Statistics screen". To obtain the definitions for the statistics presented on the Trunk Connection Statistics screen, refer to "Trunk Connection Statistics field descriptions" on page 252.

Displaying the Trunk Connection Statistics screen

Choose Alarms/Stats/Logs → Trunk Connection Statistics from the Menu Bar to display the Trunk Connection Statistics screen.

Result: Configuration Manager gathers statistics from the RLC and displays the Trunk Connection Statistics screen, similar to the example on page 250.

IF you want to	THEN click
update the statistics with the latest information,	on the **Refresh** button.
create a text file containing these statistics,	on the **Save to File** button.
close the Trunk Connection Statistics screen,	on the **Close** button.
obtain descriptions of the statistics in the Trunk Connection Statistics screen,	on the **Help** button.

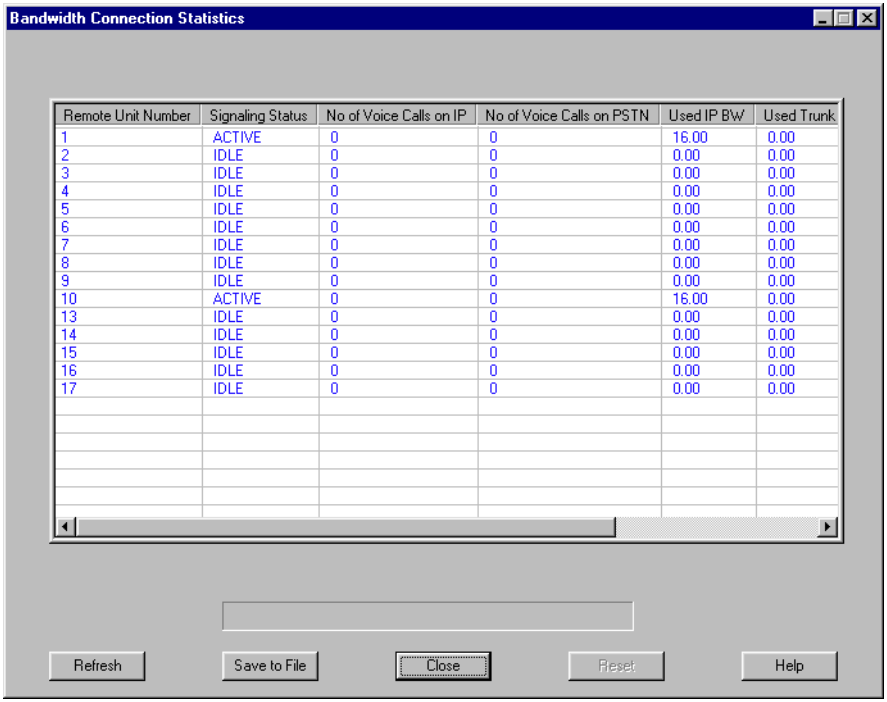
Trunk Connection Statistics field descriptions

The following table describes the statistics on the Trunk Connection Statistics screen:

Statistic	Description
Trunk Number	RLC - Identifies the Network Port number used for the call The third pair of numbers (the third item in the triplet) corresponds to the port on the RLC. 9150 - Identifies the ISDN BRI module and B-channel used for the call. 911x - Identifies the only trunk available to the remote unit with all zeroes.
Status	Identifies the current status of the trunk. Valid values are Active and Idle.
Call Type	Identifies whether the call is a local call or a remote signaling call. Valid values are Local and Signaling.
Remote ID	Identifies the remote unit involved in the call.
Called Number	Identifies the remote DN regardless of who initiated the call.
Start Time	Identifies the time that the last call on this trunk began.
Close Time	Identifies the time that the last call on this trunk ended. If the trunk is active, this statistic displays “NA”.
Duration	Identifies the amount of time taken for the call.

Bandwidth Connection Statistics

Bandwidth Connection Statistics allow you to see how much bandwidth is actually being used. These statistics help you determine if you need to add more bandwidth on the PSTN or IP network connections. They show the amount of bandwidth all remote units connected to the logged-on RLC have available to them, similar to the following:



Remote Unit Number	Signaling Status	No of Voice Calls on IP	No of Voice Calls on PSTN	Used IP BW	Used Trunk
1	ACTIVE	0	0	16.00	0.00
2	IDLE	0	0	0.00	0.00
3	IDLE	0	0	0.00	0.00
4	IDLE	0	0	0.00	0.00
5	IDLE	0	0	0.00	0.00
6	IDLE	0	0	0.00	0.00
7	IDLE	0	0	0.00	0.00
8	IDLE	0	0	0.00	0.00
9	IDLE	0	0	0.00	0.00
10	ACTIVE	0	0	16.00	0.00
13	IDLE	0	0	0.00	0.00
14	IDLE	0	0	0.00	0.00
15	IDLE	0	0	0.00	0.00
16	IDLE	0	0	0.00	0.00
17	IDLE	0	0	0.00	0.00

To display the Bandwidth Connection Statistics screen, refer to “Displaying the Bandwidth Connection Statistics screen” on page 254. To obtain the definitions for the statistics presented on the Bandwidth Connection Statistics screen, refer to “Bandwidth Connection Statistics field descriptions” on page 255.

Displaying the Bandwidth Connection Statistics screen

Choose Alarms/Stats/Logs → BW Connection Statistics from the Menu Bar to display the Bandwidth Connection Statistics screen.

Result: Configuration Manager gathers statistics from the RLC and displays the Bandwidth Connection Statistics, similar to the example on page 253.

IF you want to	THEN click
update the statistics with the latest information,	on the **Refresh** button.
create a text file containing these statistics,	on the **Save to File** button.
close the Bandwidth Connection Statistics screen,	on the **Close** button.
obtain descriptions of the statistics in the Bandwidth Connection Statistics screen,	on the **Help** button.

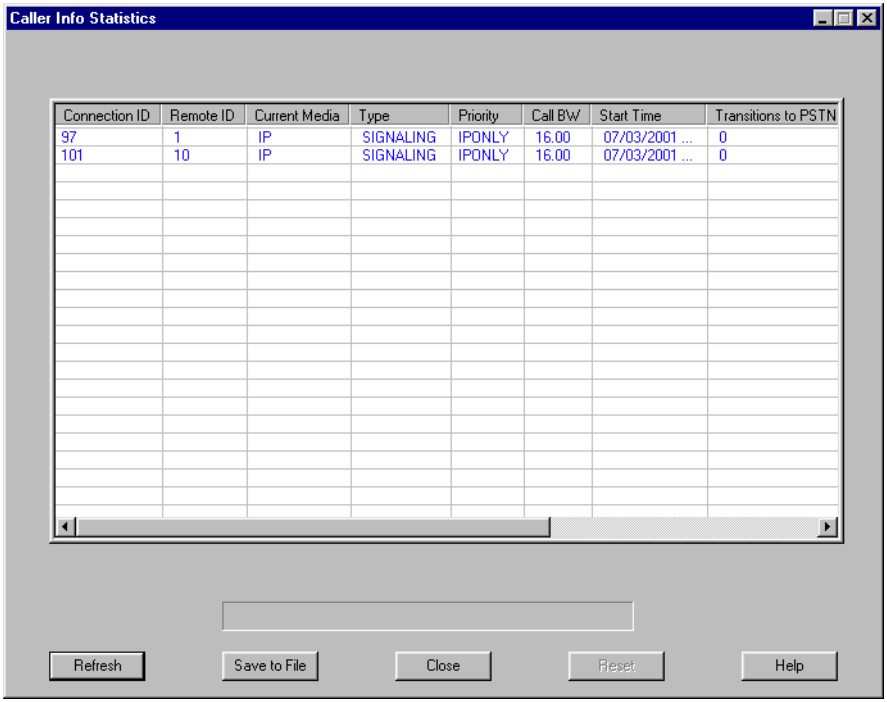
Bandwidth Connection Statistics field descriptions

The following table describes the statistics on the Bandwidth Connection Statistics screen:

Statistic	Description
Remote Unit Number	Identifies the remote unit that initiated the call.
Signaling Status	Identifies whether a connection is up on this unit. Valid values are Active and Idle.
No of Voice Calls on IP	Identifies the number of calls in progress on this unit's IP connection.
No of Voice Calls on PSTN	Identifies the number of calls in progress on this unit's PSTN connection.
Used IP BW	Identifies the IP bandwidth in use on this unit.
Used Trunk BW	Identifies the PSTN bandwidth in use on this unit.
Total Up Trunk BW	Identifies the total PSTN bandwidth up and available to this unit.
IP QoS Status	Identifies the Quality of Service (QoS) level on this unit's IP connection. Valid values are Good and Bad.

Caller Info Statistics

Caller Info (Information) Statistics show you the types of calls being made (IP or PSTN) and how often QoS transitions occur. Use these statistics to help you determine if voice QoS on your IP network is stable. The Caller Info Statistics screen is similar to the following:



To display the Caller Info Statistics screen, refer to “Displaying the Caller Info Statistics screen” on page 257. To obtain the definitions for the statistics presented on the Caller Info Statistics screen, refer to “Caller Info Statistics field descriptions” on page 258.

Displaying the Caller Info Statistics screen

Choose Alarms/Stats/Logs → Caller Info Statistics from the Menu Bar to display the Caller Info Statistics screen.

Result: Configuration Manager gathers statistics from the RLC and displays the Caller Info Statistics screen, similar to the example on page 256:

IF you want to	THEN click
update the statistics with the latest information,	on the **Refresh** button.
create a text file containing these statistics,	on the **Save to File** button.
close the Caller Info Statistics screen,	on the **Close** button.
obtain descriptions of the statistics in the Caller Info Statistics screen,	on the **Help** button.

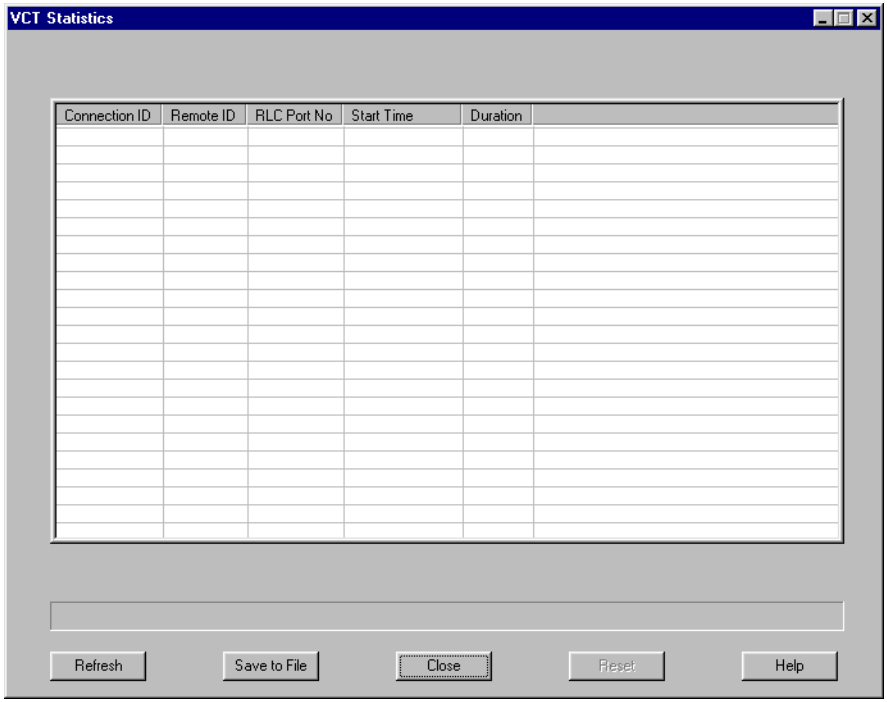
Caller Info Statistics field descriptions

The following table describes the statistics on the Caller Info Statistics screen:

Statistic	Description
Connection ID	Identifies the sequential number of the call processed by the remote unit in relation to all calls ever processed by that unit.
Remote ID	Identifies the Unit ID of the remote site that was involved in the call.
Current Media	Identifies whether the call took place over the PSTN or IP network.
Type	Identifies the type of call. Valid values are Signaling, Voice, and Local.
Priority	Identifies the priority setting of the involved trunk. Valid values are PSTN Only, IP Only, High, or Normal.
Call BW	Identifies the amount of bandwidth used by the call.
Start Time	Identifies the time that the connection initiated.
Transitions to PSTN	Identifies the number of times the RLC moved the call to the PSTN.
Transitions to IP	Identifies the number of times the RLC moved the call to the IP network.
Last Transition to PSTN	Identifies the last time the RLC moved the call from the IP network to the PSTN.
Last Transition to IP	Identifies the last time the RLC moved the call from the PSTN to the IP network.

VCT Statistics

VCT (Voice Connection Table) Statistics provide information concerning certain properties of the voice connections that are active at the time that you request the statistics. Technical support personnel use these statistics for troubleshooting purposes. The VCT Statistics screen is similar to the following:



To display the VCT Statistics screen, refer to “Displaying the VCT Statistics screen” on page 260. To obtain the definitions for the statistics presented on the VCT Statistics screen, refer to “VCT Statistics field descriptions” on page 261.

Displaying the VCT Statistics screen

Choose Alarms/Stats/Logs → VCT from the Menu Bar to display the VCT Statistics screen:

Result: Configuration Manager gathers statistics from the RLC and displays the VCT Statistics screen, similar to the example on page 259.

IF you want to	THEN click
update the statistics with the latest information,	on the **Refresh** button.
create a text file containing these statistics,	on the **Save to File** button.
close the VCT Statistics screen,	on the **Close** button.
obtain descriptions of the statistics in the VCT Statistics screen,	on the **Help** button.

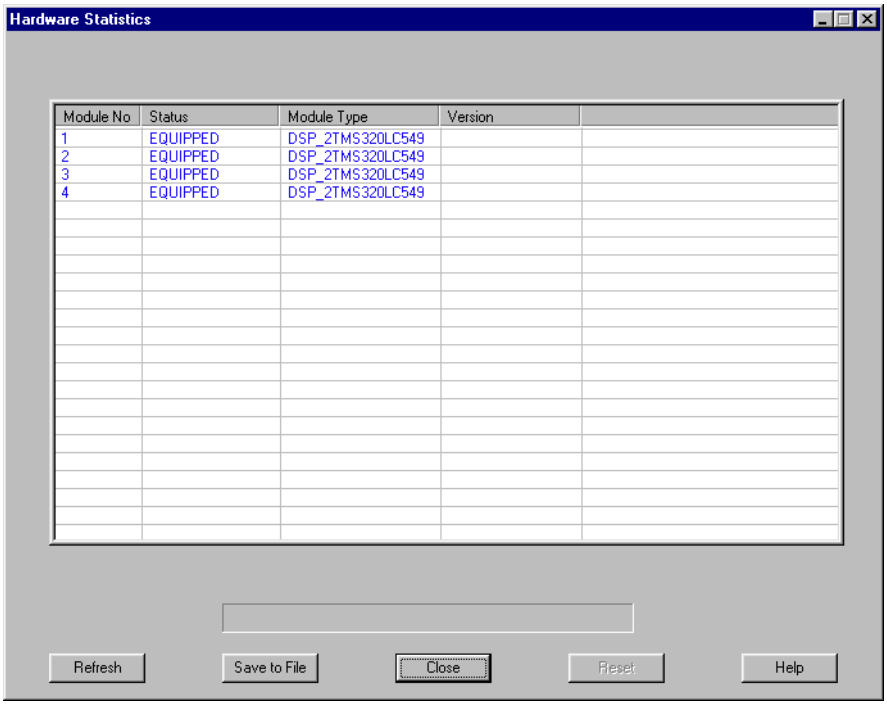
VCT Statistics field descriptions

The following table describes the statistics on the VCT Statistics screen:

Statistic	Description
Connection ID	Identifies the serial number of this call through the lifetime of the logged on unit.
Remote ID	Identifies the unit ID of the remote unit involved in the call.
RLC Port No	Identifies the port the call was processed through at the host site.
Start Time	Identifies the time and date when the call started.
Duration	Identifies how long the call lasted.

Hardware Statistics

Hardware Statistics provide information concerning the DSP application modules that are installed on the logged-on RLC. Use these statistics to determine the module positions that are populated and the type of DSP application modules present in the populated positions. The Hardware Statistics screen is similar to the following:



To display the Hardware Statistics screen, refer to “Displaying the Hardware Statistics screen” on page 264. To obtain the definitions for the statistics presented on the Hardware Statistics screen, refer to “Hardware Statistics field descriptions” on page 265.

Information concerning the DSP application modules that are installed on the RLC also appears in the Startup Information dialog box. This information includes the following:

The column	contains the following information:
SLOTNO	the slot number occupied by the application module. Valid options are 1, 2, 3, and 4.
STATUS	whether the slot contains a functioning DSP application module. Valid options are: ■ EQUIPPED—a working DSP application module is in the slot ■ OUT SERVICE—a faulty application module is in the slot ■ UNEQUIPPED—no application module is in the slot
TYPE	the type of application module in the slot
VERSION	the version of application module in the slot

This dialog box displays as the result of a successful attempt to log on to a particular RLC. You can locate the information contained in the preceding table by using the scroll bar available in the System Information section of the dialog box. Refer to page 152 for further details.

Displaying the Hardware Statistics screen

Choose Alarms/Stats/Logs → Hardware Statistics from the Menu Bar to display the Hardware Statistics screen:

Result: Configuration Manager gathers statistics from the RLC and displays the Hardware Statistics screen, similar to the example on page 262.

IF you want to	THEN click
update the statistics with the latest information,	on the **Refresh** button.
create a text file containing these statistics,	on the **Save to File** button.
close the Hardware Statistics screen,	on the **Close** button.
obtain descriptions of the statistics in the Hardware Statistics screen,	on the **Help** button.

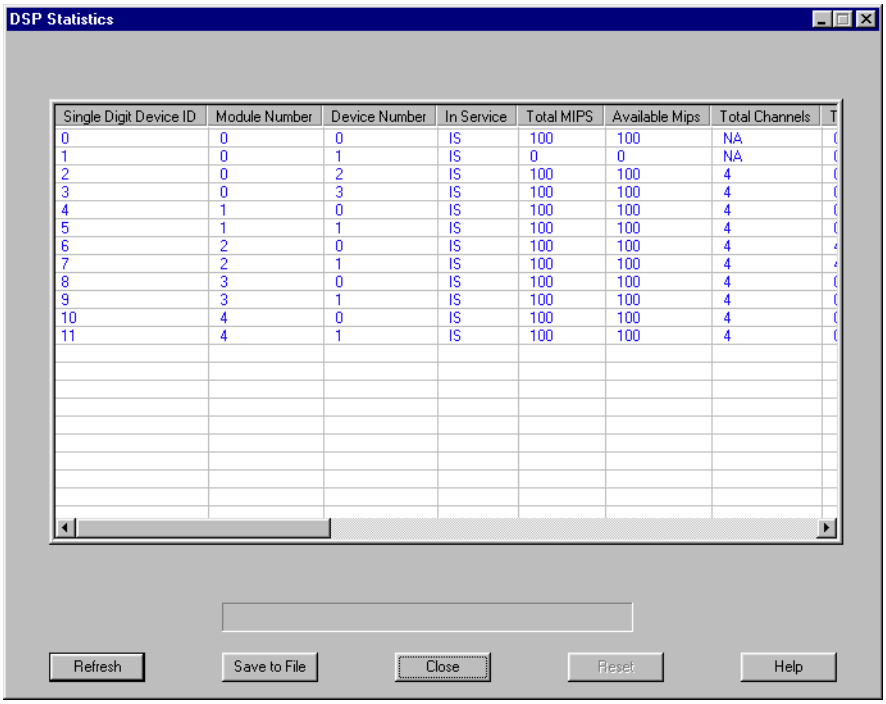
Hardware Statistics field descriptions

The following table describes the statistics on the Hardware Statistics screen:

Statistic	Description
Module No	Identifies the DSP application module's position on the RLC's motherboard.
Status	Identifies whether there is a functional DSP application module in the position identified in the Module No field. Valid values are Equipped and Unequipped. Equipped means that a DSP application module is installed in the module position and Unequipped means that there is not a DSP application module installed in the module position.
Module Type	Identifies the part number of the hardware installed in the module position.
Version	Identifies the version of DSP application module installed in the module position.

Digital Signal Processor (DSP) Statistics

Digital Signal Processor (DSP) Statistics provide information about the DSP application modules installed on the logged-on RLC. Use this screen to determine the module positions that are populated, what type of DSP those positions contain, and the functionality provided by each module. The DSP Statistics screen is similar to the following:



To display the DSP Statistics screen, refer to “Displaying the DSP Statistics screen” on page 267. To obtain the definitions for the statistics presented on the DSP Statistics screen, refer to “DSP Statistics field descriptions” on page 268.

Displaying the DSP Statistics screen

Choose Alarms/Stats/Logs → DSP Statistics from the Menu Bar to display the DSP Statistics screen:

Result: Configuration Manager gathers statistics from the RLC and displays the DSP Statistics screen, similar to the example on page 266.

IF you want to	THEN click
update the statistics with the latest information,	on the **Refresh** button.
create a text file containing these statistics,	on the **Save to File** button.
close the DSP Statistics screen,	on the **Close** button.
obtain descriptions of the statistics in the DSP Statistics screen,	on the **Help** button.

DSP Statistics field descriptions

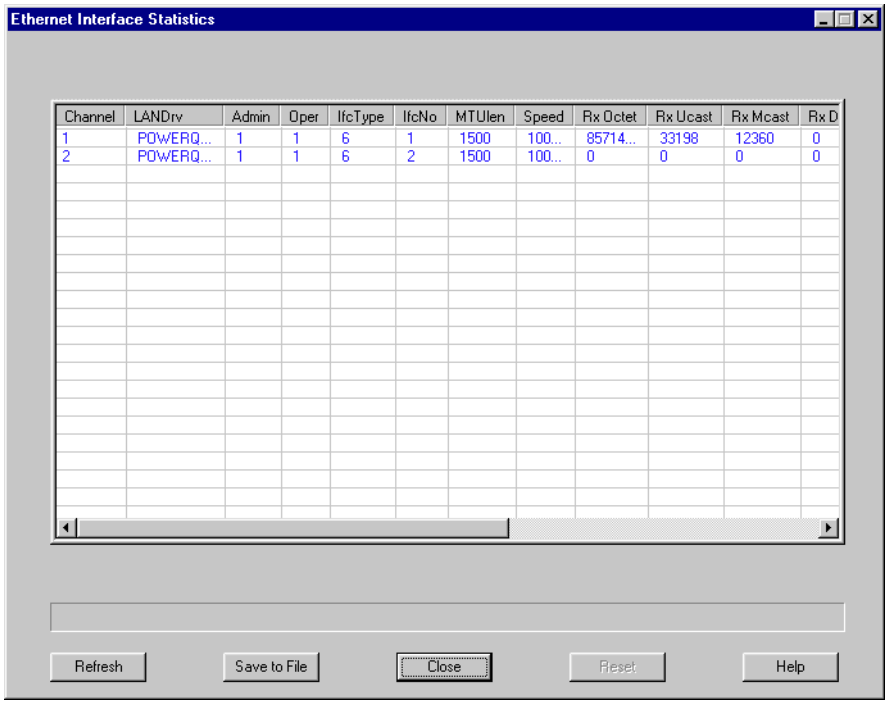
The following table describes the statistics on the DSP Statistics screen:

Statistic	Description
Single Digit Device ID	Identifies an internal sequence number for indexing this DSP device among all others on the RLC.
Module Number	Identifies this DSP Application Module's module number on the RLC. Valid values are 0, 1, 2, 3, and 4.
Device Number	Identifies the DSP device that processed the call.
In Service	Identifies any voice channels operating on this DSP application module.
Total MIPS	Identifies the total millions of instructions per second (MIPS) capacity for this DSP device.
Available Mips	Identifies the millions of instructions per second (MIPS) currently available on this DSP device.
Total Channels	Identifies the total channel capacity for this DSP device.
Total Voice Channels	Identifies the total voice channel capacity for this DSP device.
Available Voice Channels	Identifies the number of unused voice channels on this DSP device.
Total Modem Channels	Identifies the number of channels on this DSP device that can transmit modem calls.

Statistic	Description
Available Modem Channels	Identifies the number of unused channels on this DSP that can transmit modem calls.
Total Flex Channels	Identifies the number of channels on this DSP that can provide multiple functionalities.
Available Flex Channels	Identifies the number of channels on this DSP currently available to provide multiple functionalities.
Total Tones Channels	Identifies the number of channels on this DSP that can transmit tones.
Total Reserved Channels	Identifies the number of special purpose channels on this DSP reserved for internal use.
Name	Identifies the name of the DSP load, that is, the combination of DSP algorithms, on the DSP application module.

Ethernet Interface Statistics

Ethernet Interface Statistics provide information about the connection between the IP network and the logged-on RLC that is achieved over the RLC's Ethernet interface. The Ethernet Interface Statistics screen is similar to the following:



To display the Ethernet Interface Statistics screen, refer to "Displaying the Ethernet Interface Statistics screen" on page 271. To obtain the definitions for the statistics presented on the Ethernet Interface Statistics screen, refer to "Ethernet Interface Statistics field descriptions" on page 272.

Displaying the Ethernet Interface Statistics screen

Choose Alarms/Stats/Logs → Ethernet Interface Statistics from the Menu Bar to display the Ethernet Interface Statistics screen.

Result: Configuration Manager gathers statistics from the RLC and displays the Ethernet Interface Statistics screen, similar to the example on page 270.

IF you want to	THEN click
update the statistics with the latest information,	on the **Refresh** button.
create a text file containing these statistics,	on the **Save to File** button.
close the Ethernet Interface Statistics screen,	on the **Close** button.
obtain descriptions of the statistics in the Ethernet Interface Statistics screen,	on the **Help** button.

Ethernet Interface Statistics field descriptions

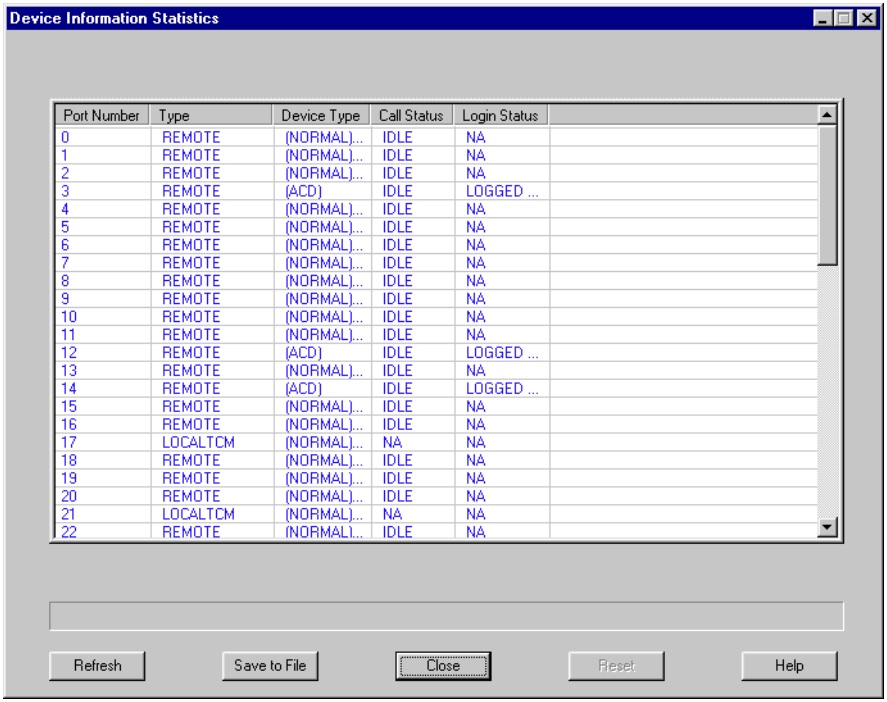
The following table describes the statistics on the Ethernet Interface Statistics screen:

Statistic	Description
Channel	Identifies the Ethernet device that the statistics on that line apply to. Valid values are 1 and 2.
LAN Drv	Identifies the LAN driver used by the call.
Admin	Identifies the desired state of the port.
Oper	Identifies the actual state of the port.
IfcType	Identifies the interface type used by the call.
IfcNo	Identifies the Ethernet interface used by the call. Valid values are 0 (ELAN) and 1 (CLAN).
MTUlen	Identifies the Maximum Transmission Unit for this interface in bytes.
Speed	Identifies the data rate of this interface in Mbps.
Rx Octet	Identifies the number of bytes received on the given channel since the statistics were last reset.
Rx Ucast	Identifies the number of packets with a unicast Ethernet address that directly matches the Ethernet address of the identified unit. This statistic describes the period of time since the statistics were last reset.
Rx Mcast	Identifies the number of multicast packets received. These packets can be broadcast MAC addresses for protocols such as ARP, as well as multicast packets for group-oriented transmissions such as IP Multicast. This statistic describes the period of time since the statistics were last reset.

Statistic	Description
Rx Disc	Identifies the number of packets discarded on the channel since the statistics were last reset.
Rx Err	Identifies the number of error packets received on the given channel since the statistics were last reset.
Tx Octet	Identifies the number of outbound bytes transmitted on the given channel since the statistics were last reset.
Tx Ucast	Identifies the number of outbound packets sent to a Unicast Address (single recipient) on the given channel since the statistics were last reset.
Tx Mcast	Identifies the number of outbound packets sent to multiple recipients on the given channel since the statistics were last reset.
Tx Disc	Identifies the number of outbound packets discarded due to resource problems on the given channel since the statistics were last reset.
Tx Err	Identifies the number of outbound packets discarded due to errors on the given channel since the statistics were last reset.
QLen	Identifies the number of bytes currently in the interface's outbound queue.
Collisions	Identifies the number of collisions that have occurred on the Ethernet interface while attempting to transmit packets since the statistics were last reset. **Note:** The Collisions statistic appears on both the Ethernet Interface and Network Statistics screens. The Collisions statistic is only applicable in half-duplex mode.

Device Information Statistics

Device Information Statistics provide information about the device connected to each port of the logged-on RLC, similar to the following:



To display the Device Information Statistics screen, refer to “Displaying the Device Information Statistics screen” on page 275. To obtain the definitions for the statistics presented on the Device Information Statistics screen, refer to “Device Information Statistics field descriptions” on page 276.

Displaying the Device Information Statistics screen

Choose Alarms/Stats/Logs → Device Information from the Menu Bar to display the Device Information Statistics screen.

Result: Configuration Manager gathers statistics from the RLC and displays the Device Information Statistics screen, similar to the example on page 274.

IF you want to	THEN click
update the statistics with the latest information,	on the **Refresh** button.
create a text file containing these statistics,	on the **Save to File** button.
close the Device Information Statistics screen,	on the **Close** button.
obtain descriptions of the statistics in the Device Information Statistics screen,	on the **Help** button.

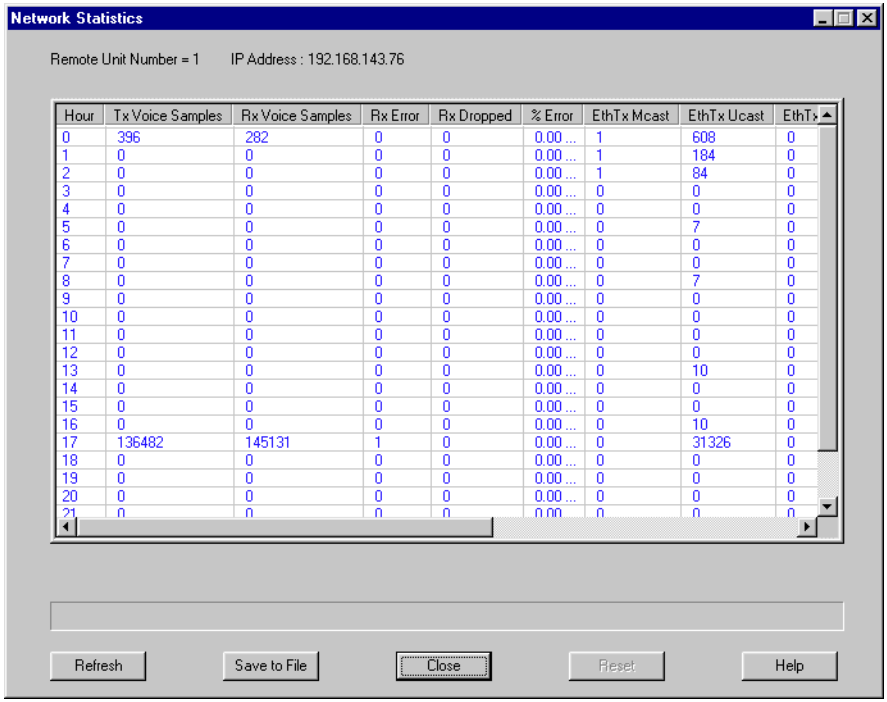
Device Information Statistics field descriptions

The following table describes the information on the Device Information Statistics screen:

Statistic	Description
Port Number	Identifies the RLC port number associated with the displayed information.
Type	Identifies the port type. Valid values are Remote, Data, and Local TCM.
Device Type	Identifies whether the telephone connection on the port identified is Normal or ACD. Valid values are Normal and ACD.
Call Status	Identifies whether the port is currently handling a call. Valid values are Busy and Idle.
Login Status	Identifies whether the telephone connected to this port is active on the system. Valid values are Logged on and Logged off. **Note:** This statistic applies only to ports associated with ACD telephones.

Network Statistics

Network Statistics allow you to see the performance over the last 24 hours of the remote units connected to the logged-on RLC. Use these statistics to identify periods when other network activity can adversely affect Remote Office system performance. This screen shows remote unit performance in terms of the transmission and reception of frames and packets, similar to the following.



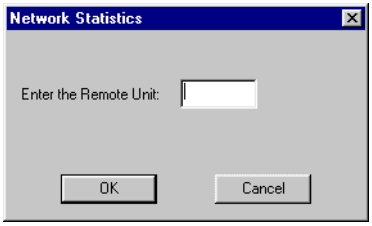
Hour	Tx Voice Samples	Rx Voice Samples	Rx Error	Rx Dropped	% Error	EthTx Mcast	EthTx Ucast	EthTx
0	396	282	0	0	0.00 ...	1	608	0
1	0	0	0	0	0.00 ...	1	184	0
2	0	0	0	0	0.00 ...	1	84	0
3	0	0	0	0	0.00 ...	0	0	0
4	0	0	0	0	0.00 ...	0	0	0
5	0	0	0	0	0.00 ...	0	7	0
6	0	0	0	0	0.00 ...	0	0	0
7	0	0	0	0	0.00 ...	0	0	0
8	0	0	0	0	0.00 ...	0	7	0
9	0	0	0	0	0.00 ...	0	0	0
10	0	0	0	0	0.00 ...	0	0	0
11	0	0	0	0	0.00 ...	0	0	0
12	0	0	0	0	0.00 ...	0	0	0
13	0	0	0	0	0.00 ...	0	10	0
14	0	0	0	0	0.00 ...	0	0	0
15	0	0	0	0	0.00 ...	0	0	0
16	0	0	0	0	0.00 ...	0	10	0
17	136482	145131	1	0	0.00 ...	0	31326	0
18	0	0	0	0	0.00 ...	0	0	0
19	0	0	0	0	0.00 ...	0	0	0
20	0	0	0	0	0.00 ...	0	0	0
21	0	0	0	0	0.00	0	0	0

To display the Network Statistics screen, refer to “Displaying the Network Statistics screen” on page 278. To obtain the definitions for the statistics presented on the Network Statistics screen, refer to “Network Statistics field descriptions” on page 279.

Displaying the Network Statistics screen

1 Choose Alarms/Stats/Logs → Network Statistics from the Menu Bar to display the Network Statistics screen.

Result: Configuration Manager prompts you for the unit ID of the remote unit that you want to check Network Statistics for, similar to the following:



2 Enter the Unit ID.

3 Click on the **OK** button.

Result: The Network Statistics screen displays, similar to the example on page 277.

IF you want to	THEN click
update the statistics with the latest information,	on the **Refresh** button.
create a text file containing these statistics,	on the **Save to File** button.
close the Network Statistics screen,	on the **Close** button.
obtain descriptions of the statistics in the Network Statistics screen,	on the **Help** button.

Network Statistics field descriptions

The following table describes the information on the Network Statistics screen:

Note: A *decoder packet* is a nominal DSP voice packet. The size of a decoder packet varies according to the compression algorithm used. Decoder packets can be added to a superpacket before the DSP forwards the superpacket to the host.

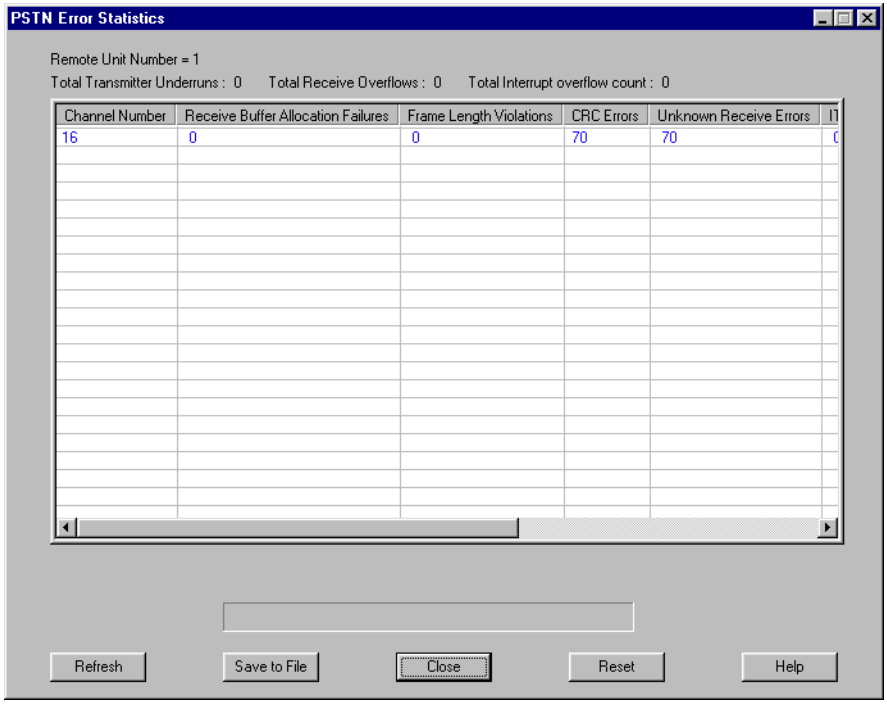
Statistic	Description
Hour	Identifies the 60-minute period, within the most recent 24 hours, that the other statistics on this line apply to. The statistics on the line where "0" is in this column refer to activity that occurred within 60 minutes of the request for statistics. The statistics on the line where "1" is in this column refer to activity that occurred during the 60-minute period that ended 60 minutes, or one hour, before the request for statistics. The statistics on the line where "2" is in this column refer to activity that occurred during the 60-minute period that ended two hours before the request for statistics, and so on.
Tx Voice Samples	Identifies the number of decoder packets transmitted by the DSP during the given hour. This number corresponds to in-band signaling, such as DTMF or Fax Relay, and voice signaling transmitted by the DSP. **Note:** This statistic formerly was expressed in superpackets rather than decoder packets.
Rx Voice Samples	Identifies the number of decoder packets received by the DSP during the given hour. This number corresponds to in-band signaling, such as DTMF or Fax Relay, and voice signaling received by the DSP. **Note:** This statistic formerly was expressed in superpackets rather than decoder packets.
Rx Error	Identifies the number of decoder packet overruns and underruns during the given hour, as determined by the DSP.

Statistic	Description
Rx Dropped	Identifies the number of superpackets that were received out of sequence during the given hour. This can result from one or more superpacket's being lost or delivered out of order and, thus, discarded.
%Error	Identifies the packet error percentage that was received during the given hour. Remote Office begins calculating this statistic by adding the number out-of-sequence packets (Rx Dropped) to the number of overruns. After multiplying this sum by 100, Remote Office then divides the product by the number of received decoder packets (Rx Voice Samples) to produce the error percentage. This is an imprecise measurement due to the fact that multiple packet losses or overruns can be counted as a single error.
EthTx Mcast	Identifies the number of multicast packets transmitted during the given hour. Multicast packets are packets intended for multiple Ethernet addresses.
EthTX Ucast	Identifies the number of unicast packets transmitted during the given hour. Unicast packets are packets intended for a specific Ethernet address. Voice packets are always transmitted as unicast packets.
EthTx Disc	Identifies the number of packets discarded on the transmit side due to lack of resources, such as memory buffers, during the given hour. This can be an indirect result of excessive collisions in the transmit queue.
EthTx Err	Identifies the number of packets that could not be transmitted because of errors within the packets.

Statistic	Description
EthRx Mcast	Identifies the number of multicast packets that were received during the given hour. This is inclusive of packets with broadcast MAC addresses for protocols such as ARP, and multicast packets for group-oriented transmissions, such as IP Multicast. Multicast packets are packets intended for more than one Ethernet address.
EthRx UCast	Identifies the number of unicast packets that were received during the given hour with a unicast Ethernet address directly matching that of the specified unit. Unicast packets are packets intended for only one Ethernet address.
EthRx Disc	Identifies the number of packets that were received during the given hour and discarded due to a lack of available receive buffers.
EthRx Err	Identifies the number of packets that were received during the given hour that contained errors that prevented them from being deliverable to a higher-layer protocol.
Collisions	Identifies the number of collisions that have occurred on the Ethernet interface when attempting to transmit packets since the statistics were last reset. **Note:** The Collisions statistic appears on both the Ethernet Interface and Network Statistics screens. It is only applicable in half-duplex mode.

PSTN Error Statistics

PSTN Error Statistics allow you to see the PSTN performance, in terms of signaling errors, of remote units connected to the logged-on RLC. Use these statistics to indicate the effectiveness of your connection to the PSTN. The table displays error totals for all active PSTN calls from the specified remote unit, similar to the following.

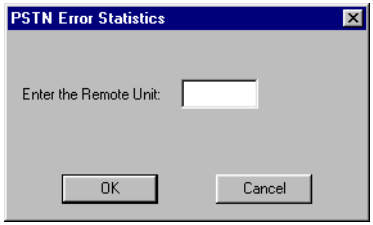


Note: PSTN Error Statistics are only available for Remote Office 9150 units.

Displaying the PSTN Error Statistics screen

1 Choose Alarms/Stats/Logs → PSTN Error Statistics from the Menu Bar to display the PSTN Error Statistics screen.

Result: Configuration Manager prompts you for the unit ID of the remote unit that you want to check PSTN Error Statistics for, similar to the following:



2 Enter the Unit ID.

3 Click on the **OK** button.

Result: The PSTN Error Statistics screen displays, similar to the example on page 282.

IF you want to	THEN click on the
update the statistics by adding PSTN error information that occurred since your original request,	**Refresh** button.
create a text file containing these statistics,	**Save to File** button.
close the PSTN Error Statistics screen,	**Close** button.
begin collecting new statistics,	**Reset** button.
obtain descriptions of the statistics in the PSTN Error Statistics screen,	**Help** button.

PSTN Error Statistics field descriptions

The following table describes the information on the PSTN Error Statistics screen:

Statistic	Description
Channel Number	Identifies the channel that the statistics on that line apply to.
Receive Buffer Allocation Failures	Identifies the number of times since the statistics were last reset that there was an error in the allocation of a packet to the receive buffer.
Frame Length Violations	Identifies the number of times since the statistics were last reset that a frame contained too many packets.
CRC Errors	Identifies the number of times since the statistics were last reset that the cyclic redundancy check (CRC) bits did not match. The CRC errors that Trunk Protocol reports on the Remote Office product are check performed end-to-end at the High-level Data Link Control (HDLC) framing level. This check includes the ISDN framing errors as well as PSTN spans and clocking issues. The CRC error count does not always indicate that there are CRC errors on the physical line between the RLC and the CO, or the host PBX and the CO. However, the CRC error count is a good indication that you need to investigate the physical line.
Unknown Receive Errors	Identifies the number of times since the statistics were last reset that a receive error that is not otherwise classified in this display occurred.
ITE Frame Length Violations	Identifies the number of times since the statistics were last reset that the ITE received an over-length frame.
ITE Transmitter Underruns	Identifies the number of times since the statistics were last reset that the ITE transmitter contained underruns.
ITE Receive Busy Errors	Identifies the number of times since the statistics were last reset that the ITE received busy errors.

Verifying the firmware and software version

This section describes how to determine the version of firmware and software currently installed.

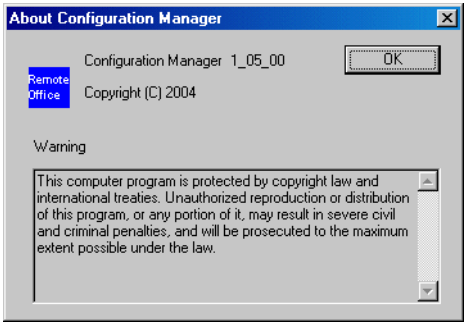
Before you perform a firmware or software upgrade, determine the version that is currently installed. This ensures that you do not replace the installed firmware or software with an older version.

Verifying the software version

To verify the software version on your RLC:

1 From the Menu Bar, choose Help → About Configuration Manager.

Result: The About Configuration Manager dialog box displays, similar to the following:



2 Review the About Configuration Manager dialog box. This identifies the version of software installed on the unit.

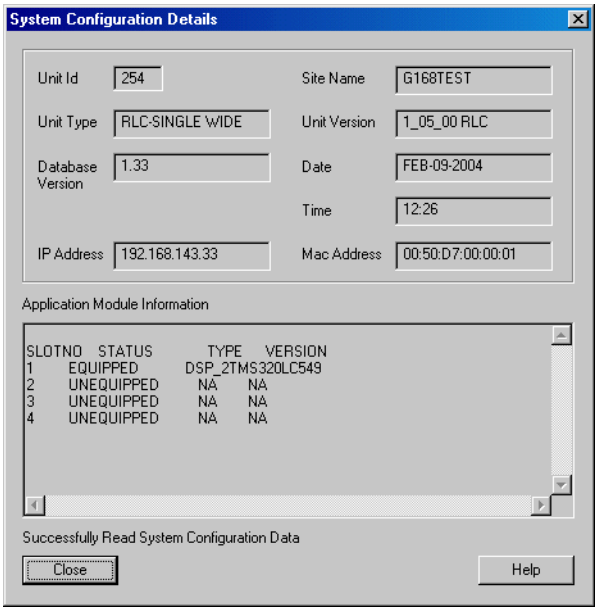
3 Click on the **OK** button.

Verifying the firmware version

To verify the firmware version on your RLC:

1 From the Menu Bar, choose System Information → System Data.

Result: The System Configuration Details dialog box displays, similar to the following:



2 Review the Unit Version field. This identifies the version of firmware installed on the unit.

3 Click on the **Close** button.

Determining the current firmware and software versions

To determine what the current firmware and software versions are, refer to the *Remote Office and RLC Release Notes* (NTP 555-8421-102).

Obtaining the latest upgrade file

If you need to upgrade the firmware or software, you can obtain the latest upgrade files by clicking on the Software Downloads link at the following website:

www.nortelnetworks.com

Nortel Networks provides upgrade files in self-extracting executable files. You must extract the upgrade files before you can perform the upgrade.

Types of upgrades

You can perform the following types of upgrades for your RLC:

- Configuration Manager software upgrade

  You use Configuration Manager software to configure or administer the RLC.
- firmware upgrade for the RLC motherboard
  The firmware contains the code necessary for operating the RLC.

  Note: This includes any firmware updates that have been made for DSP application modules.

Downloading the upgrade file

To download the upgrade file:

1. With your web browser, connect to the Nortel Networks website at:

   www.nortelnetworks.com
2. Click on the **Software Downloads** link.
3. Locate the software and firmware you need.
4. Download the files into a temporary location on your PC.
5. Double-click on the **.exe** file to extract the files into a temporary location on your PC.

Performing a firmware upgrade

This section describes how to perform a firmware upgrade on your RLC. You perform the upgrade over the IP network using the TFTP protocol. You can perform the RLC upgrade manually or configure the RLC to perform an automatic or scheduled firmware upgrade. Refer to “Auto upgrade configuration” on page 228 for further details.

You must have a TFTP server application running on the administration PC. Ensure that the TFTP server’s base directory points to the directory that contains the upgrade files.

Manual firmware upgrade

To ensure trouble-free communication between the RLC and Remote Office units during and after the manual firmware upgrade, Nortel Networks recommends that you perform the upgrades as follows:

1. Create backup configuration files for the Remote Office 9150, Remote Office 911x series, and Meridian Digital Telephone IP Adapter units and for the RLC. Refer to “Creating a backup configuration file” in the Nortel Networks Installation and Administration Guide for the specific product.
2. Upgrade the Configuration Manager software on the administration PC.
3. Disable the PBX slot(s) where an RLC is installed.
4. Upgrade the RLC firmware.
5. Upgrade the Remote Office 9150, Remote Office 911x series, and Meridian Digital Telephone IP Adapter unit firmware.
6. Remote Office 9150 units only - Upgrade the BRI module firmware for each BRI module.
7. Restart the RLC.
8. Restart all upgraded Remote Office units.
9. Re-enable the PBX slot(s) where an RLC is installed.

Note: Upgrade the Remote Office 9150 unit’s firmware before upgrading the Remote Office 9150 unit’s BRI module firmware.

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, refer to “Verifying the firmware and software version” on page 285.

ATTENTION

The protocol for communication between the RLC and the Remote Office units requires that they be running the same version in order for them to communicate with each other.

About firmware upgrades and configuration files

Each time you perform a firmware upgrade, the configuration database also converts (if necessary) to a format that is compatible with the new firmware. The conversion does not affect configuration settings.

Nortel Networks recommends that each time you perform a firmware upgrade, you first create a backup copy of the converted configuration file and store it in a safe, secure location.

Before you begin

It is important to complete the following steps before performing a firmware upgrade:

1. Obtain the firmware upgrade from Nortel Networks.

   For instructions, refer to “Obtaining the latest upgrade file” on page 287.
2. Extract the upgrade files from the file you received from Nortel Networks.
3. Start the TFTP server application.
4. Ensure the TFTP base directory reflects the directory where the firmware upgrade file you want to use resides.

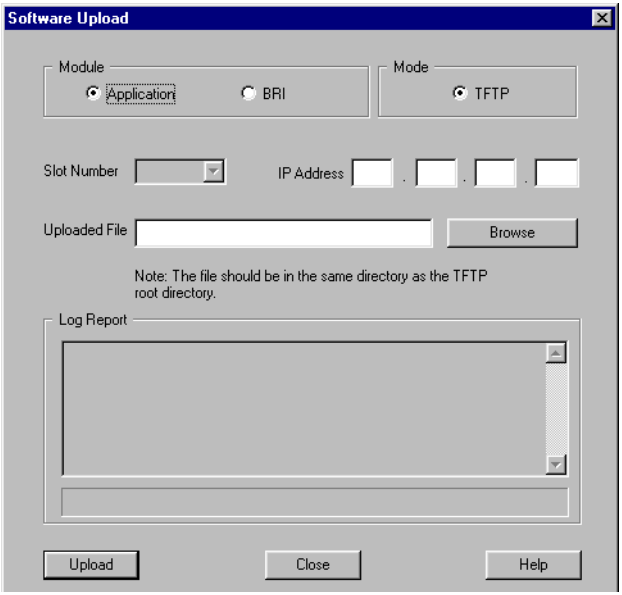
Getting there RLC → Configuration Manager

Upgrading the RLC firmware

To upgrade the RLC firmware:

1 From the Menu Bar, choose Upload/Download → Upload S/W.

Result: The Software Upload dialog box displays, similar to the following:



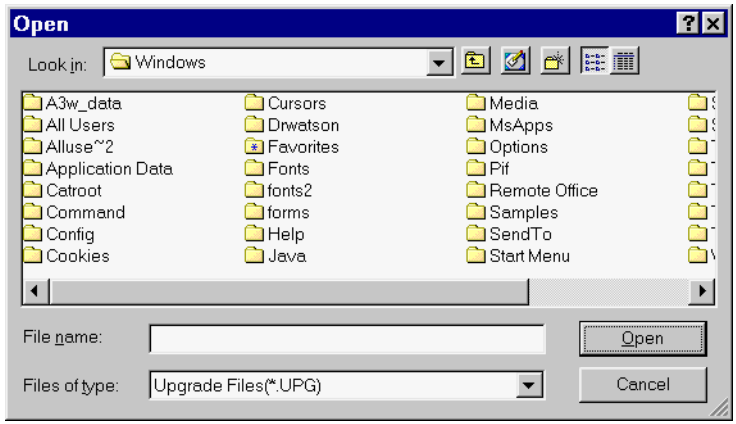
2 In the Module section, click on the **Application** option button.

3 Enter the IP address of the TFTP server in the IP Address fields.

Note: Since the TFTP server application runs on your administration PC, this is the IP address of the PC.

4 Click on the **Browse** button.

Result: The Open dialog box displays, similar to the following:



5 Ensure the Files of type drop down box shows Upgrade Files(*.UPG).

6 Navigate to the folder where the firmware file is located.

7 Select the file, and then click on the **Open** button.

Example: Select rlc-100.upg, and then click on the **Open** button.

Result: The Software Upload dialog box re-displays. The file you selected is shown in the Uploaded File field.

8 Click on the **Upload** button.

Wait until the file uploads completely before entering any other commands. The Log Report window displays a confirmation message when the upgrade is complete.

9 Restart the RLC.

Automatic or scheduled firmware upgrade

When you configure the RLC to perform an automatic or scheduled firmware upgrade using the Auto Upgrade Configuration property sheet, the RLC queries the predefined TFTP server and upgrades the firmware automatically. Refer to “Auto upgrade configuration” on page 222 for further details.

USE CAUTION WHEN FORCING THE AUTO UPGRADE PROCESS AS THE SYSTEM PERFORMS A SELF-RESET ON ALL UNITS TO MAKE THE NEW FIRMWARE ACTIVE ONCE THE DOWNLOAD OF NEW FIRMWARE IS COMPLETE.

Nortel Networks recommends the following when performing an automatic or scheduled firmware upgrade:

1. Complete the procedures in “Before you begin” on page 289 prior to configuring the automatic or scheduled upgrade.
2. Complete the procedures in “Creating a backup configuration file” on page 238 before performing an automatic or scheduled firmware upgrade.

Note: The automatic or scheduled firmware upgrade only performs upgrades on the Remote Office units you configure on the Auto Upgrade Configuration property sheets.

Self-contained firmware upgrade

A self-contained firmware upgrade executable file is also available.

To perform this form of upgrade, both the administration PC and the RLC must be connected using a 10BaseT Ethernet connection. The self-contained firmware upgrade executable file can run on a Windows 98, NT Workstation 4.0, Millennium Edition (ME), 2000 Professional, or XP (Professional and Home Edition) operating system.

To obtain the self-contained firmware upgrade executable file, click on the **Software Downloads** link at the following website:

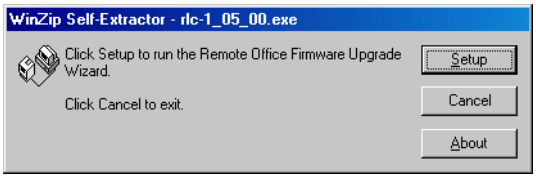
www.nortelnetworks.com

Note: You can also email this file to a remote user.

To perform the upgrade:

1 Double click on the .exe file.

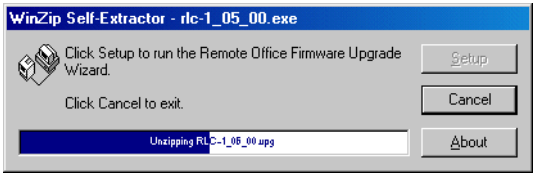
Result: The WinZip Self-Extractor dialog box displays, similar to the following:



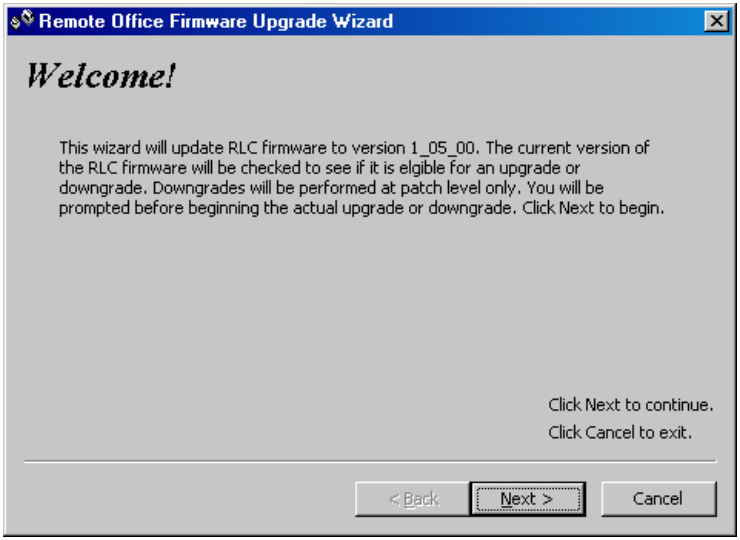
2 Click on the **Setup** button to run the Remote Office Firmware Upgrade Wizard.

Note: You can cancel the upgrade at anytime by clicking on the Cancel button on any of the upcoming dialog boxes. You can find out information regarding this application by clicking on the About button.

Result: The WinZip Self-Extractor unzips the RLC upgrade file and displays an unzip progress bar, similar to the following:

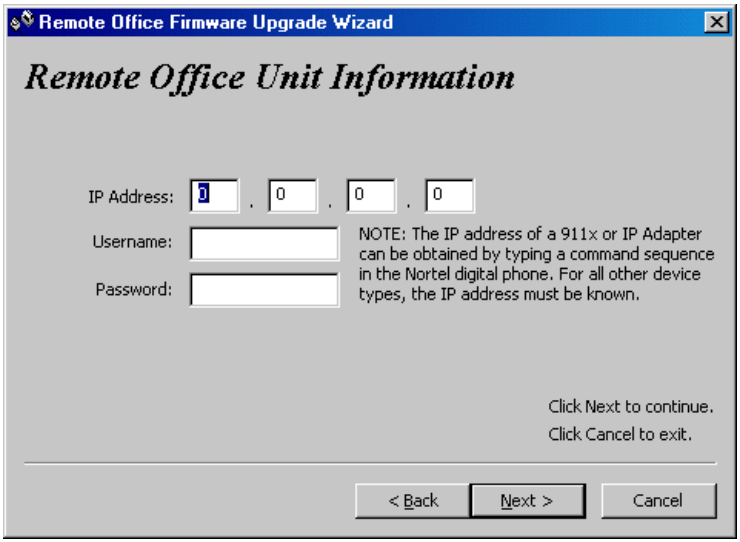


3 Once the unzip process is complete, the Welcome dialog box displays, similar to the following:



4 Click on the **Next** button.

Result: The Remote Office Unit Information dialog box displays, similar to the following:



5 Enter the IP address of the RLC that you want to upgrade.

6 Enter your logon name in the Username field. If you have not yet customized this setting, refer to “Default logon ID and password” on page 149 for the default logon ID.

7 Enter your password in the Password field. If you have not yet customized this setting, refer to “Default logon ID and password” on page 149 for the default password.

8 Click on the **Next** button and follow the instructions on the upcoming dialog boxes to complete the upgrade process.

After successful installation, the executable file removes all residual files excepting the executable itself. For the RLC, the self-contained firmware upgrade application issues a software-reset command in order to make the new firmware active.

Performing a software upgrade

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, refer to “Verifying the firmware and software version” on page 285.

Upgrading the Configuration Manager software

To upgrade the Configuration Manager software:

1. Navigate to the directory that contains the upgrade files you extracted.
2. Locate and double-click on the **setup.exe** file.
3. Follow the prompts on screen.

ATTENTION

Do not ignore any warning messages the InstallShield displays about versions of files (such as DLL files) that already exist on your PC. If you overwrite these files, you may inadvertently cause other applications on your PC to stop working.

Result: The InstallShield installs the software, overwriting the previous version.

Chapter 8

Troubleshooting

In this chapter

Before you begin

If you experience problems in setting up or running your RLC, this chapter can help you to isolate and solve the problem.

Identifying why a problem occurred

Before you begin, ask yourself the questions listed in the following table:

Question	IF you answered	THEN do the following steps
Is this a new installation?	yes,	Perform troubleshooting in the sequence presented in this chapter.
	no,	Answer the next question.
Did the RLC work, 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,	Verify that changes were made correctly. Check the hardware components to ensure they are working correctly. Perform troubleshooting for the specific component the problem appears in.
	no,	Contact your telecom or data network administrator. There may be a problem with the network.

Reach Line Card LED indicators

The Reach Line Card (RLC) LED indicators give you an indication of the line card's general health. When you reset your RLC, correct LED indicator behavior is as follows:

- The Maintenance LED behavior upon card insertion:
  - — lights solid
  - — flashes three times after completing self-test

    Note: The self-test takes approximately 60 seconds.

  - — goes off after the host PBX enables the RLC

    Note: During normal operation of the RLC, the Maintenance LED remains off.
- The remaining LED indicators flash when there is network activity.

What to do if the LEDs do not display correctly

The following table describes what to do if the LEDs do not display correctly:

Symptom	What to do
The Maintenance LED did not flash three times during the power-up cycle.	**1** Reset the RLC. Watch the Maintenance LED again. Approximately 60 seconds pass before it flashes. **2** If the Maintenance LED still does not flash, contact your Nortel Networks distributor. There may be a hardware problem.
The Maintenance LED is lit after a successful self-test.	**1** Check to see if the slot is enabled on the host PBX. **2** If other LED indicators are not lit or flashing, did the Maintenance LED ever light? If not, contact your Nortel Networks distributor. There may be a hardware problem. **3** Ensure that the RLC is properly seated in its slot and is properly inserted into the backplane. If the Maintenance LED remains lit, contact your Nortel Networks distributor. There may be a hardware problem.
The Maintenance LED is flashing.	The power-up self-test failed. Contact your Nortel Networks distributor. There may be a hardware problem.
No LED indicators are lit on the RLC.	**1** Ensure that the slot the RLC resides in has power applied. **2** Ensure that the RLC is properly seated in its slot. If the RLC is properly seated in its slot and no LED indicators light, contact your Nortel Networks distributor. There may be a hardware problem.

Symptom	What to do
The Ethernet COLL LED is lit solid when Half-Duplex Ethernet is enabled in the IP configuration.	Network collisions are bound to occur and are normal. However, if the Ethernet COLL LED is lit solid when Half-Duplex Ethernet is enabled in the IP configuration, complete the following steps: **1** Check the physical network connection. **2** Verify that the RLC can be PINGed. **3** Check the network configuration (such as routing, traffic load, and so on). Adjust the network configuration, if required. **4** Normally, there is 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.

Network connectivity

This section identifies some problems that can occur on the 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:

Symptom	What to do
You cannot establish a connection from your administration PC to the RLC.	**1** Ensure that you entered the IP address correctly when trying to establish the connection. **2** Ensure that you entered the logon name and password correctly when trying to establish the connection. **3** Ensure the RLC's IP address, network mask, and default gateway are configured correctly on the RLC. **4** PING the RLC. **5** PING the gateway. **6** If the PING still does not work, contact your data network administrator.

Symptom	What to do
`10060 TELNET CONNECTION FAILED` appears when attempting to connect to the RLC.	**1** Ensure that you entered the IP address correctly when trying to establish the connection. **2** Ensure that you entered the logon name and password correctly when trying to establish the connection. **3** Ensure that no one is already logged on to the RLC. **4** Verify that the Ethernet cable is connected at both ends (RLC and network hub). **5** Check the Ethernet cable and ensure it is good. **6** Ensure the RLC is properly seated in its slot. **7** Verify that the IP address, subnet mask and gateway are all correct on the RLC. **8** PING the RLC. **9** If the RLC does not respond, PING the RLC's gateway to see if it responds. **10** If the gateway does not respond, PING a known good device on the RLC's network. **11** If steps 9 and 10 work, but step 8 did not, there may be a gateway configuration error. Check the unit's IP Configuration property sheet. **12** If the problem still exists, contact your Nortel Networks distributor. There may be a hardware problem.

Symptom	What to do
SERIAL CONNECTION FAILED appears when attempting to connect to the RLC.	**1** Ensure that you entered the logon name and password correctly when trying to establish the connection. **2** Ensure that someone is not already logged on to the RLC. **3** Ensure the RLC is properly seated in its slot. **4** Reseat the RLC. **5** Ensure you specified the correct COM port when attempting the connection. **6** Verify that no other applications on the administration PC are using the COM port. **7** Check the serial cable connection to ensure it is good. **8** Using a breakout box, verify that the COM port is active. **9** If the problem still exists, contact your Nortel Networks distributor. There might be a hardware problem.
The RLC does not send or receive Ethernet traffic.	**1** Ensure the RLC is seated in its slot properly and connected to the backplane. **2** Check the Ethernet cable between the RLC and the network and ensure it is good. **3** Ensure the Ethernet cable is connected. **4** If the RLC still does not send or receive traffic, contact your data network administrator. **5** Data network administrator: Ensure other network devices are configured to allow traffic to and from the RLC.

Symptom	What to do
An attempt to log off from the RLC does not work.	It is possible that the administration PC and the RLC have lost communication with one another. Close Configuration Manager, then restart it.
The RLC cannot establish a connection with the remote unit.	IP or PSTN installations: **1** Verify security authentication configuration and ensure that it matches at both ends. (For example, if using security identifier, ensure that the inbound and outbound security identifiers are correctly configured at each end.) **2** Ensure that the unit IDs are configured correctly at each end. An incorrect unit ID causes security authentication to fail. **3** Verify that the PSTN and IP networks are operational (up and running) as appropriate to your location. **4** Ensure that the RLC is enabled on the host PBX.

Symptom	What to do
The RLC cannot establish a connection with the remote unit. (continued)	Additional steps for IP-only installations: **1** Confirm that the RLC's IP address and PSTN number are correctly configured on the remote unit. Also confirm that correct remote unit configuration exists at the host site. **2** Use the PING option in Configuration Manager to PING the remote unit. For instructions, refer to "Performing a Configuration Manager PING," on page 312. **3** If the remote unit does not respond, check the network configuration (such as, routing, traffic load, and so on). Adjust the network configuration, if required. Additional steps for PSTN only installations: **1** Verify that network ports are configured on the host PBX, one for each BRI channel that is to provide remote connectivity. **2** Verify that the 9150 PSTN telephone number is configured correctly on both the Remote Connection Configuration property sheet (refer to "Remote connection configuration" on page 197) and the BRI Configuration property sheet (refer to "Configuring BRI Trunks" in the *Remote Office 9150 Installation and Administration Guide* NTP 555-8421-215). **Note:** This is the same telephone number configured on both property sheets.

Symptom	What to do
The RLC cannot establish a connection with the remote unit. (continued)	**3** Verify that the network port PSTN telephone number is configured correctly on both the Network Port Configuration window of the RLC Port Configuration property sheet (refer to "Configuring an RLC port" on page 188) and "Configuring the RLC Connection information" in the *Remote Office 9150 Installation and Administration Guide* NTP 555-8421-215). **Note:** This is the same telephone number configured on both property sheets.

Software problems

This section identifies some problems that can occur with the Configuration Manager software, and describes what to do to resolve them.

Symptom descriptions

If you are not able to complete a task with Configuration Manager, perform troubleshooting as described in the following table:

Symptom	What to do
The Configuration Manager software installation fails.	Ensure that you close all background applications, including anti-virus checking software before performing the installation.
When performing one of the following by TFTP, `ERROR: FILE OPEN FAILED` displays: ■ configuration upload ■ RLC firmware upgrade	**1** Ensure the TFTP server application is installed and running on your administration PC. **2** Ensure the file you are trying to upload is present in the target directory. That is, either in the TFTP directory, or in the directory that is specified as the base directory in the TFTP server application. **3** Review messages displayed by the TFTP server application for clues. **4** PING the remote 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 an RLC configuration file.

Symptom	What to do
`CONFIG UPLOAD FAILED` when attempting to perform a configuration upload by TFTP. (continued)	**2** Ensure that the configuration file you are attempting to upload is compatible with current RLC firmware. **3** Perform the configuration upload using a previous configuration file, if necessary. **Note:** Each time you perform a RLC firmware upgrade, create a backup of the configuration. The configuration database format in the RLC is dependent on the version of firmware installed on the RLC. If you recently downgraded to a previous version of RLC firmware, you may 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 unit. Close Configuration Manager, and then restart it.
Nothing happens when attempting to log off from the RLC.	It is possible that communication has been lost between the administration PC and the node you were logged on to. Close Configuration Manager, and then restart it.

Display Logs definitions

You can locate Display Logs definitions in the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215) and Configuration Manager online Help.

QoS testing

This section identifies problems that can occur during QoS testing when using IP connectivity as the main method of connectivity, with PSTN connectivity for QoS transition. This section also describes what to do to resolve the problem.

Symptom descriptions

If the Remote Office system does not make the transition to the PSTN connection when you disconnect the Ethernet cable (or the network goes down), perform troubleshooting as described in the following table:

Symptom	What to do
The connection does not transfer from the IP network to the PSTN when the Ethernet connection is broken.	**1** Ensure that you selected PSTN:Status:**Enable** on the Remote Connection Configuration property sheet for the connection in question. ■ Ensure that the PSTN number of the remote unit is entered in the PSTN Number field on the same property sheet. ■ Ensure that the port number of the Dedicated Network Port is entered in the Dedicated PSTN n/w Port field on the same property sheet. **2** Ensure that the Dedicated PSTN n/w Port mentioned above is configured as a network port on the RLC Port Configuration property sheet. ■ Ensure that the appropriate PBX Data port is configured and enabled.

Symptom	What to do
The connection does not transfer from the IP network to the PSTN when the IP connection is lost. (continued)	**3** Ensure that “Type:Remote” or “Type:Local & Remote” and “Status:Enable” are selected for each active BRI channel (refer to “Configuring BRI Trunks” in the *Remote Office 9150 Installation and Administration Guide* NTP 555-8421-215). **4** Ensure that you selected “Status:Enable” in the Quality of Service window of the Remote Connection Configuration property sheet (refer to “Remote connection configuration” on page 197). Verify that the Signal Degrade slide in the same window is set to an acceptable level (refer to “Configuring QoS” on page 211). **5** Understand that the QoS monitoring process monitors the network through sampling, according to the QoS Threshold slider settings. For testing purposes only, set the sliders to the far right and select one second in the Duration:Signal Degrade field.

Using Configuration Manager PING

PING, or Packet InterNet Groper, is a protocol and program to test whether a device is accessible on a network. This section explains how to use the PING option provided in Configuration Manager to verify connectivity. Use this procedure as a troubleshooting tool to determine if you can reach the remote unit, another RLC, or any other device on the network.

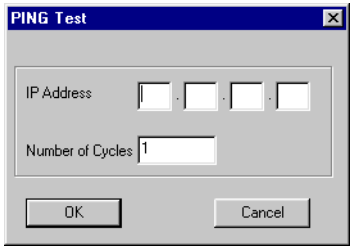
Getting there RLC → Configuration Manager

Performing a Configuration Manager PING

To perform a Configuration Manager PING:

1 From the Menu Bar, choose Tests → Ping.

Result: The PING Test dialog box displays, similar to the following:

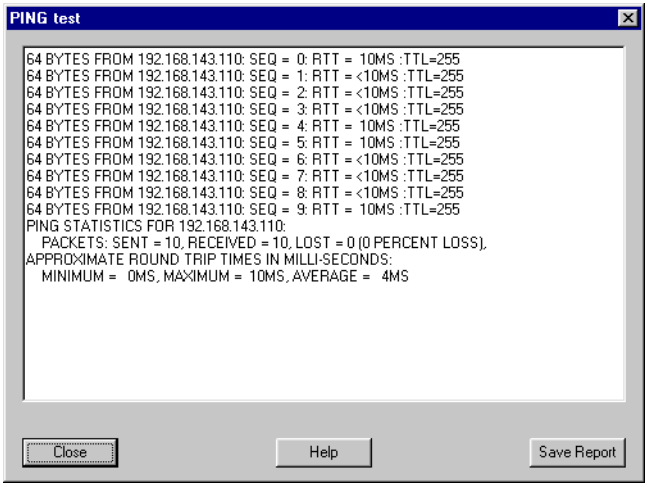


2 Enter the IP Address of the unit you want to PING in the IP Address field.

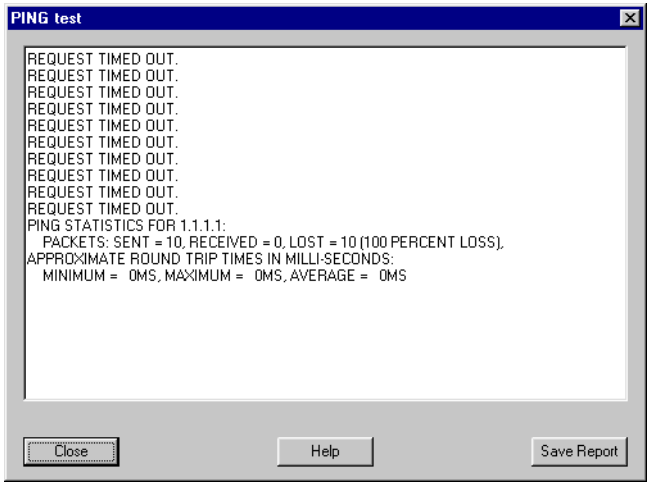
3 Enter the number of times you want to PING the unit in the Number of Cycles field (1 to 100).

4 Click on the **OK** button.

Result: The PING test window displays, showing the PING results. The following is an example of a successful PING.



The following is an example of an unsuccessful PING.



5 Click on the **Close** button.

Result: The PING test window closes.

ATTENTION

It is possible to successfully PING a device on the network and still not be able to log on to that device. If you log on to a device (an RLC) using a serial connection and neglect to log off, you may be able to successfully PING the device but be unable to establish a Telnet connection to it. (The device believes itself to be busy.)

If you cannot log on to a device after a successful PING, access the serial port and ensure that you are not logged on to the device through this port.

Unsuccessful PING options

If the PING was unsuccessful:

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

PSTN connectivity testing

Use the PSTN Connectivity command to ensure that PSTN configuration is correct. On initial installations, ensure that you have entered all required information. On established installations, look for problems with the PSTN connection. Use the command to indicate potential sources for problems.

Notes:

1. When performing a PSTN connectivity test on a Remote Office 9150 unit, the test only checks the primary ISDN connection outbound from the RLC. It does not check the primary connection inbound to the RLC from the Remote Office 9150 unit's BRI circuit. The only way to verify an initial primary PSTN connection from the Remote Office 9150 unit is to manually initialize the *primary* link from the Remote Office 9150 unit.

   PSTN connectivity tests always use the configured Trunk Support speed.

2. When performing a PSTN connectivity test on a Remote Office 911x series unit, the test only checks the primary PSTN connection to and from the RLC.

To avoid common configuration mistakes, Nortel Networks recommends that you test the PSTN operation after you have finished configuring the PSTN numbers. In addition, Nortel Networks further recommends that you only do PSTN testing during periods when the Remote Office unit is NOT in use.

PSTN connectivity tests work in two modes:

- Disruptive mode

  Note: If your Remote Office 911x series unit is operating in PSTN only mode, you must perform PSTN connectivity testing in disruptive mode.

- Non-disruptive mode

In both cases, you can perform the tests on a specified Remote Office unit for a specified range of data ports on the RLC. When using the disruptive mode, Nortel Networks recommends that you wait two or three minutes between tests to give the Remote Office system time to recover.

You can abort the PSTN tests at any time and return the system to normal operation mode. The start and end of PSTN tests are recorded as display logs. To view these display logs, access Configuration Manager → Alarms/Logs/Stats → Display Logs.

WARNING During PSTN testing, do not make any configuration changes or perform a Save to Flash on the RLC or Remote Office unit involved in the PSTN testing.

If the system reports that it cannot perform PSTN tests, determine the following:

1. Is the PSTN enabled on the Remote Office unit?
2. Is the Remote Office unit enabled?

Note: During testing, the system reports the status of the test on each RLC port.The meaning of each status message is shown in the following table:

No	Status Message	Comments
1	Trunk up	Link was brought up successfully to the specified number and Meridian unit port.
2	Attempt Failed	Attempt made to call specified number failed.
3	Port Busy	The specified port is in use and cannot be tested.
4	No Remote Port Available	There is no Meridian unit port available to bring up trunk on specified port.
5	Security Failed	There was a security failure while bringing up the trunk. Check security configuration settings.
6	Abnormal Failure	There is an abnormal failure on this connection due to errors on the line or an emergency call on the Remote Office 9150 unit.
8	Not Closed	In non-disruptive mode, this trunk bandwidth is being used for voice calls and could not be freed.
9	Primary not up	If the primary trunk can not be brought up, all additional trunks show this status.
10	Primary Abnormal Fail	All additional trunks show this message if the primary trunk experiences an abnormal failure during testing.
11	Not data port	The specified port is not configured as a data port.
12	Attempt by Remote Failed	Attempt by the Meridian unit to bring up trunks from remote side failed.

13	Closed	During normal testing process, this message indicates that a trunk brought up for testing purpose closed normally.
14	No Number to Dial	Displayed for primary if there is no PSTN number configured to dial Remote Office 9150 unit, or if the primary port is in use. Check PSTN number configuration and try to do test at a later time.
15	Primary to another unit	The specified port is primary to another Meridian unit. No test can be performed on this port.

Disruptive mode testing

If any voice calls are present on the PSTN when the testing starts, Disruptive mode testing causes all existing PSTN lines to the specified Remote Office unit to close abruptly. Before the test starts, however, the system displays a warning message indicating the number of voice calls present. You must specify that you want to go ahead with the tests.

In addition, on the Remote Office 9150 unit:

- Local trunk calls that have occupied Local and Remote configured B-channels drop.
- Remote calls occupying Remote configured B-channels drop.
- Local calls occupying Remote configured B-channels and Emergency 911 calls do not drop.
- You cannot place any local outgoing trunk calls on trunk groups that use Local and Remote B-channels.
- Similarly, no incoming local trunk calls are allowed on Local and Remote B-channels.

During disruptive mode testing, the following occurs:

- A primary channel is brought up from the RLC side.
- Other channels are tested from the:
  - — RLC to the Remote Office 9150 unit
  - — Remote Office 9150 unit to RLC in the given range of data ports of the RLC
- QoS transition is not allowed to happen.
- No voice calls are allowed to go on the PSTN.

- The start and end of PSTN tests are recorded as display logs. To view these display logs, access Configuration Manager → Alarms/Logs/Stats → Display Logs.
- The user can abort the PSTN tests at any time and system returns to normal operation mode.

Non-disruptive mode testing

Non-disruptive mode tests do not disturb the operation of your system. The system functions normally in that:

- Calls from Meridian units on PSTN can be made.
- QoS transition occurs.
- Remote Office 9150 unit local trunks calls (both incoming and outgoing) are allowed (including emergency calls).

In addition:

- You may observe that some PSTN lines brought up during the testing process do not drop automatically.
- Sometimes ports that have not been brought up during testing, but were closed due to the release of PSTN bandwidth are shown as released if they are in the given range. This depends on how many calls are placed on PSTN while test is in progress.
- It may not be possible to test some trunks by bringing them up from the RLC or Remote Office 9150 unit and vice versa if they are already in use.

Troubleshooting

If after running the PSTN tests you encounter any PSTN failures, review Chapter 4, “Configuring the host PBX for the RLC” on 107.

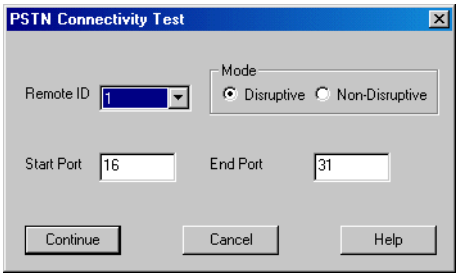
Getting there RLC → Configuration Manager

Performing PSTN connectivity testing

To test your remote unit's PSTN connections:

1 From the Menu Bar, choose Tests → PSTN Connectivity.

Result: The PSTN Connectivity Test dialog box displays, similar to the following:



2 Select the Remote ID of the unit that you want to check the PSTN connection on from the Remote ID drop down list box.

3 Do one of the following:

- Click on the **Disruptive** option button for tests performed at initial installations or after-hours when you can shut down the entire system.
- Click on the **Non-Disruptive** option button for tests performed during business hours or any time when you cannot shut down the entire system.

4 Enter the port number of the first port that you want to test PSTN connectivity on in the Start Port field.

5 Enter the port number of the last port that you want to test PSTN connectivity on in the End Port field.

6 Click on the **OK** button.

When the test is complete, the unit presents a log with test results and statistics.

Syslog testing

Once you configure the Syslog feature and save it to Flash, use the Syslog test command to test the configuration. The Remote Office system generates test syslog messages. This allows you to verify the syslog configuration as well as the syslog collector functionality on the syslog server(s).

Getting there RLC → Configuration Manager

Performing syslog testing

To perform syslog testing:

1 From the Menu Bar, choose Tests → Syslog.

Result: A message displays, similar to the following:

2 Click on the **OK** button.

3 Examine the syslog server(s) to see if the test was successful.

Alarms and alerts

For troubleshooting purposes, each Remote Office device transmits alarms and alerts to the host PBX. These alarms and alerts indicate to the host PBX that the Remote Office device is in a state of alarm or alert. The host PBX then produces an alarm or alert through its software. Refer to “Display Logs” in the *Remote Office 9150 Installation and Administration Guide* (NTP 555-8421-215) or Configuration Manager online Help to determine if the host PBX produces an alarm or alert when Remote Office Configuration Manager produces a display log.

Responding to a catastrophic failure

For the purposes of this discussion, a *catastrophic failure* is defined as a failure of the equipment to operate after review of all troubleshooting information and implementation of appropriate procedures.

Inoperative hardware

If your RLC fails to operate after thorough review of the troubleshooting information in this and related Guides, consult your Nortel Networks distributor for hardware replacement.

Repair and warranty information

The RLC contains no user-serviceable components. If the problem experienced with your RLC persists after you have used all the appropriate procedures in this chapter, refer to the following contact information for repair and warranty help, depending upon your location.

Note: If the RLC is causing harm to the telephone network, the telephone company may request that you disconnect it pending resolution of the problem.

Canada

Nortel Networks Service Selection Center
30 Norelco Drive
Weston, ON
Canada
M9L 2X6

Telephone: 1-800-466-7835

United States

Nortel Networks
Product Service Center
640 Massman Drive
Nashville, TN 37210
USA

Telephone: 1-800-466-7835

Europe

Nortel Networks (NI) Ltd.
FAO: Irish Express Cargo (IEC)
Raheen Industrial Estate
Raheen, Limerick
Ireland

Telephone: 00 800 8008 9009 or +44 (0) 870 907 9009
Fax: +33 4 9296 1598

Asia/Pacific

Nortel Distribution Center
c/o ACCO Transport
21 South St. Unit#2
Rydalmere, NSW
2116 Australia

CALA

Note: When you need warranty and repair service in Central American and Latin American countries, you must first get an RR (repair and return) number from your Nortel Networks distributor before shipping to the Nortel CALA Repair Center.

Nortel c/o Wesbell
4019 S.W. 30th Avenue
Fort Lauderdale, FL 33312
USA
Notify: Receiving Department
RR no.:

Telephone:
Normal Service Hours (Monday through Friday, 8:00 a.m. to 5:00 p.m. Central Time): 1-954-851-8841
After Normal Hours (weekends and holidays): 1-888-594-8474

Fax: 1-954-581-2334

Appendix A

Planning forms

In this appendix

Completing the RLC forms

ATTENTION Before you can assign RLC ports to remote users, you must determine the total remote user requirements for the RLC.

To complete the forms:

1 Assign users on the remote units to remote ports on the RLC.

Note: To do this effectively, obtain information from the configuration information forms for all remote units connected to this RLC.

Record the RLC port assignments in the “Port configuration” section on one of the following RLC forms (according to the type of RLC installed):

- Connection Information—16 ports
- Connection Information—32 ports

Users who are using an MCA to transmit data must be assigned to a PBX data port. Users who are using ATAs can be assigned to PBX voice or data ports. Configure ATA users as voice ports only if there are not enough free data ports. Refer to “Remote port configuration” on page 112 for more information.

Note: The Connection Information forms identify the maximum number of ports that can be associated with MCAs and ATAs that are used to transmit data.

2 If you want to route calls over the PSTN, designate 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 unit.

Note: You must assign Network ports to PBX data ports.

Record the network port assignments and remote unit PSTN numbers on the Connection Information form for your RLC type.

3 Record the IP address for each remote unit on the Connection Information form for your RLC type.

4 If the chosen security level is provisioned security, record the security identifier that each remote unit uses to validate connection requests.

Note: You must configure the same security level on both the RLC and remote unit.

5 On the same form, record the following items for the 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 an RLC Online/Offline Table Configuration form for each remote unit.

Reach Line Card

Connection Information—16 ports

Complete one copy of this form for each line card. **Page 1 of 5**

RLC information

IPE position: Loop:_____ Shelf: _____ Card:_____

IP address: ___.___.___.___

Subnet mask: ___.___.___.___

Default gateway: ___.___.___.___

Host PBX's ELAN IP address: ___.___.___.___

Host PBX's ELAN subnet mask: ___.___.___.___

Security level: ❒ No security is required ❒ Caller ID ❒ Provisioned Security*

*If the security level is *provisioned security,* RLC's security identifier:

Inbound _____

Outbound _____

Notes:

- This RLC provides 32 total ports. Ports 0–15 are Voice ports and ports 16–31 are Data ports. On the host PBX, you must configure Network ports or Remote ports that use MCAs or ATAs (for data transmission) as Data ports. If there are not enough free Data ports, you can configure Remote ports that use ATAs as Voice ports. You can configure Remote ports used for FAX support as either Voice ports or Data ports. Refer to documentation for your PBX for necessary procedures.
- QoS Transition Technology requires one MCA per B-channel.
- If you want to use MCAs or ATAs to transmit data, you can connect a maximum of four MCAs or ATAs to Remote ports on this RLC.

Reach Line Card

Connection Information—16 ports

Port configuration

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
0	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
1	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
2	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
3	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
4	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
5	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
6	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
7	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
8	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			

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	Security ID (if Network port)
9	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
10	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
11	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
12	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
13	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
14	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
15	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
16	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
17	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			

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	Security ID (if Network port)
18	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
19	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
20	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
21	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
22	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
23	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
24	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
25	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
26	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			

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	Security ID (if Network port)
27	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
28	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
29	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
30	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			
31	❒ Network ❒ Remote ❒ Local TCM	❒ Yes ❒ No			

Reach Line Card

Connection Information—32 ports

Complete one copy of this form for each Line Card. **Page 1 of 9**

RLC information

IPE position: Loop:_____ Shelf: _____ Card:_____

IP address: ___.___.___.___

Subnet mask: ___.___.___.___

Default gateway: ___.___.___.___

Host PBX's ELAN IP address: ___.___.___.___

Host PBX's ELAN subnet mask: ___.___.___.___

Security level: ❒ No security required ❒ Caller ID ❒ Provisioned Security*

*If the security level is *provisioned security*, RLC's security identifiers:

Inbound _____

Outbound _____

Notes:

- This RLC provides 64 total ports. Ports 0–31 are Voice ports and ports 32–63 are Data ports. On the host PBX, you must configure Network ports or Remote ports that use MCAs or ATAs (for data transmission) as data ports. If there are not enough free data ports, you can configure Remote ports that use ATAs as voice ports. You can configure Remote ports used for FAX support as either voice ports or data ports. Refer to documentation for your PBX for necessary procedures.
- QoS Transition Technology requires one MCA per B-channel.
- If MCAs or ATAs are to be used to transmit data, a maximum of seven MCAs or ATAs can be connected to this Reach Line Card.

Reach Line Card

Connection Information—32 ports

Port configuration **Page 2 of 9**

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
Slot 1					
0	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
1	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
2	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
3	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
4	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
5	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
6	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
7	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
8	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			

Reach Line Card

Connection Information—32 ports

Port configuration (continued) **Page 3 of 9**

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
9	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
10	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
11	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
12	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
13	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
14	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
15	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
16	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
17	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			

Reach Line Card

Connection Information—32 ports

Port configuration (continued) **Page 4 of 9**

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
18	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
19	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
20	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
21	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
22	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
23	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
24	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
25	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
26	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			

Reach Line Card

Connection Information—32 ports

Port configuration (continued) **Page 5 of 9**

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
27	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
28	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
29	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
30	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
31	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			

Reach Line Card

Connection Information—32 ports

Port configuration (continued) **Page 6 of 9**

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
Slot 2					
32	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
33	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
34	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
35	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
36	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
37	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
38	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
39	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
40	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			

Reach Line Card

Connection Information—32 ports

Port configuration (continued) **Page 7 of 9**

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
41	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
42	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
43	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
44	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
45	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
46	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
47	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
48	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
49	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			

Reach Line Card

Connection Information—32 ports

Port configuration (continued) **Page 8 of 9**

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
50	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
51	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
52	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
53	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
54	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
55	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
56	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
57	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
58	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			

Reach Line Card

Connection Information—32 ports

Port configuration (continued) **Page 9 of 9**

RLC port number	Port type	MCA, ATA, or FAX?	PSTN number (if Network port)	IP address	Security ID (if Network port)
59	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
60	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
61	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
62	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			
63	❒ Network ❒ Remote ❒ Local telephone	❒ Yes ❒ No			

Reach Line Card

Online/Offline Table Configuration

Page 1 of 1

RLC unit number: *254* 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								

Reach Line Card

System expansion worksheet

Number of DSP application modules needed

Complete one worksheet for each RLC.

1 How many simultaneous faxes do you want your equipment to support?

Multiply the number of simultaneous faxes by two to determine the total number of DSP channels required for fax calls. (Each fax call requires two DSP channels.)

_____ x 2 = _____ _____

Note:

- If the number of DSP channels required for fax calls is not divisible by four, round up the number entered in step 1 to the next multiple of four. (Each DSP device contains four channels.) Always round up to a higher number.

2 Divide your Step 1 answer, the total number of DSP channels required for fax calls, by four to determine the number of DSP devices required for fax calls. (Configuration Manager assigns DSP function on a per-device basis.)

Step 1: _____ / 4 = _____ _____

Reach Line Card

System expansion worksheet

Number of DSP application modules needed (continued)

3 How many remote users do you want to support?

Notes:

- Up to 16 users can be connected to the NTDR68xx Line Card. Up to 32 users can be connected to the NTDR70xx or NTDR71xx Line Cards.
- If using ATAs or MCAs to transmit data, the NTDR68xx Line Card supports up to four ATAs or MCAs. NTDR70xx or NTDR71xx Line Cards support up to seven ATAs or MCAs. Each ATA requires the resources of one DSP channel for data transmission.

_____

4 Do you want to implement call blocking? (Users will receive a fast busy signal when resources are not available.) ❒ Yes ❒ No

5 If step 4 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 your step 3 answer 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 your step 1 answer by 2/3 (0.666). If the result contains a fraction, round up to a whole number.

Step 3: _____ x _____ = _____

If step 4 is No, the number of simultaneous calls is the same as the number of user stations installed. (Record your response to step 3 here.)

_____

Reach Line Card

System expansion worksheet

Number of DSP application modules needed (continued)

6 Divide your step 5 answer by 8, then round down the result to a whole number.
Step 5: _____ / 8 = _____ _____

The total number of DSP channels required at the local site equals the total number of simultaneous remote service telephone calls that you want to allow on your entire remote network. This includes calls from Remote Office 9150, 9110, 9115 units, and Meridian Digital Telephone IP Adapter units (Internal and External). Assuming that there are eight voice channels available on a single DSP application module (the current DSP application module channel capacity), and taking into account the eight built-in DSP channels on the RLC and Remote Office 9150 unit, determine the number of DSP application modules required on your host PBX using the following equations:

A: fax DSP devices required =
simultaneous fax calls from Remote Office 9150 / 2
(This calculation assumes G.729/FAX compression. For G.711 or G.726, divide by four.)

B: voice DSP devices required =
simultaneous remote service voice calls required for 9150 and 911x / 4

C: 911x DSP devices required =
simultaneous PSTN connections for 911x / 4

total DSP devices required = A + B + C - 2

Note: Each DSP application module consists of two DSP devices.

Reach Line Card

System expansion worksheet

Number of DSP application modules needed (continued)

(step 6 continued) If the result of equations A or B is a fraction, round *up* to the nearest whole number. For example, for a simultaneous combination of 2 fax calls, 17 remote service telephone calls and 0 PSTN connections for 911x, the equations are as follows:

A: fax DSP devices required = 2 / 2= 1

B: voice DSP devices required = 17 / 4= 4.25 = 5

(For 17 remote service calls, the equation works out to 4.25 and rounds up to five.)

C: 911x DSP devices required = 0 / 4 = 0

total DSP required = 1 + 5 + 0 - 2 = 4
total DSP application modules required = 2

A remote network supporting 2 fax and 17 remote service telephone calls simultaneously requires two DSP application modules. If the RLC supports more than one remote site, remember that its DSP application modules must support the voice processing for all sites combined.

7 Record the number of DSP application modules already installed.

Note: The RLC shipped from Nortel Networks with one DSP module built in. Your response here must include that module. _____

8 Calculate how many DSP modules you need to purchase.
Subtract your step 7 answer from your step 4 answer.

Note: Only four DSP application modules can be installed on the NTDR68xx Line Card. Up to four DSP application modules can be installed on the NTDR70xx or NTDR71xx Line Cards. _____

9 Record the number of DSP application modules already installed.

Note: The RLC shipped from Nortel Networks with one DSP module built in. Your response here must include that module. _____

Reach Line Card

System expansion worksheet

Number of DSP application modules needed (continued)	
10 Calculate how many DSP modules you need to purchase. Subtract your step 7 answer from your step 4 answer. **Note:** Only four DSP application modules can be installed on the NTDR68xx Line Card. Up to four DSP application modules can be installed on the NTDR70xx or NTDR71xx Line Cards.	_____
11 Allow for future growth?	❒ Yes ❒ No
Note: All users at a Remote Office 9150 site must be assigned to one RLC only. Therefore, future assignment of RLC ports should be considered. For example, if a Remote Office 9150 site grows from 8 to 20 users, and 12 more ports are not available on the RLC, then you must reassign of the entire Remote Office 9150 site (20 users) to another RLC.	

Appendix B

Sample configuration files

In this appendix

Example of a network

This section provides an example of a network diagram that shows one host site (with one 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 352
- data port for Remote Office 9150 unit: on page 354
- data port for Remote Office 911x series unit: on page 356

Sample configuration printouts for the RLC, Remote Office 9150 unit, and Remote Office 911x series unit are shown as follows:

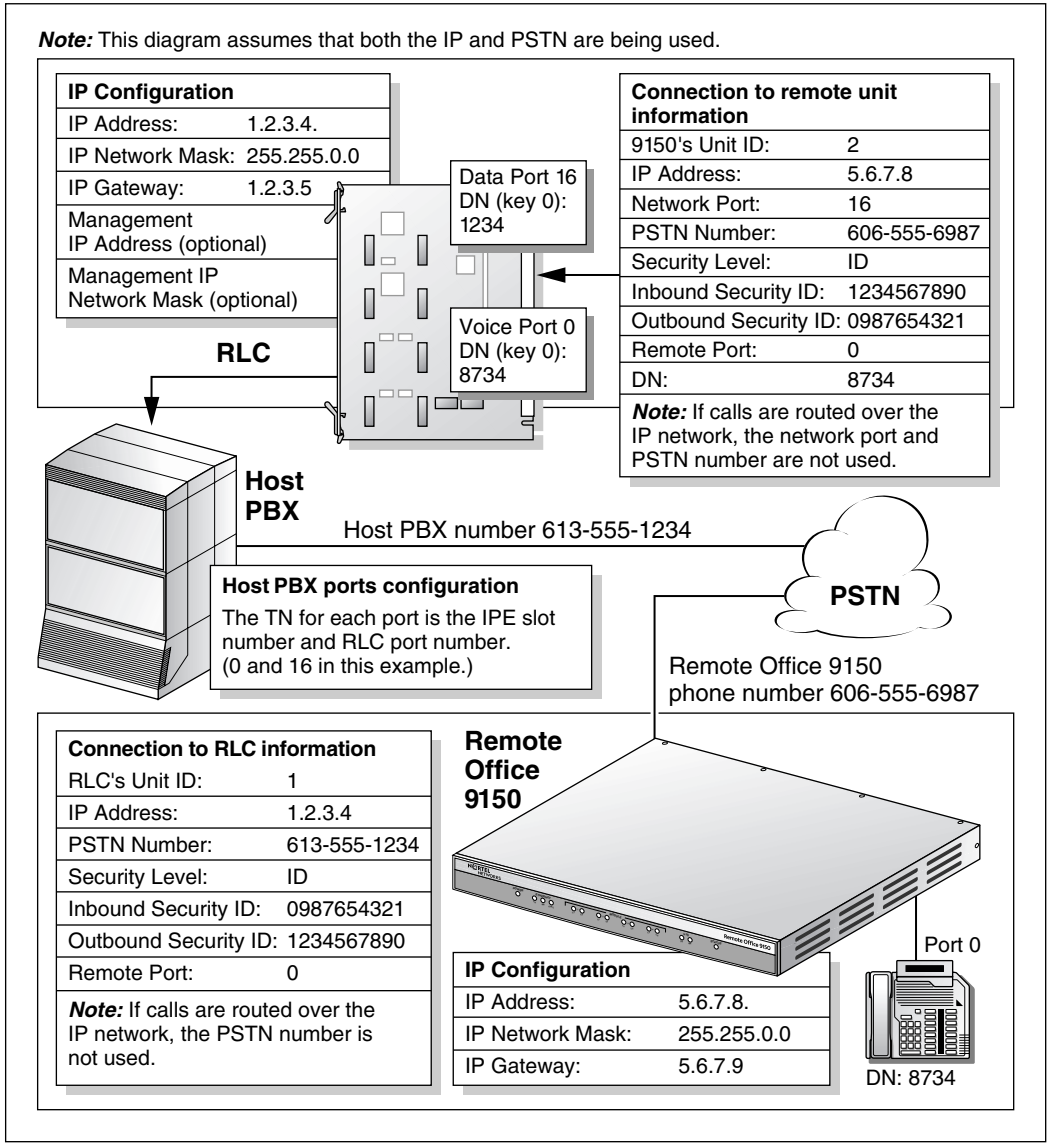
- RLC: on page 365
- Remote Office 9150 unit: on page 369
- Remote Office 911x series unit: on page 372

Configuration recommendation

The quickest way to configure the RLC, Remote Office 9150 unit, and Remote Office 911x series unit is to run the Configuration Wizard. For instructions, refer to “Using the Configuration Wizard to perform initial configuration” on page 92. 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

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 351.

Note: This configuration example is from a Meridian 1 PBX 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

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.

User's DN

User's CPND

Data port configuration for 9150 on the Meridian 1 PBX

This section shows the configuration settings for the data port on the Meridian 1 PBX. The data port provides the communication path between the RLC and the Remote Office 9150 unit, and must be configured as an MCA.

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 351.

Note: This configuration sample is from a Meridian 1 PBX 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

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 56000
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.

Baud defaults to 56K, however, the RLC determines actual Baud on a per-call basis.

The number that the Remote Office 9150 unit needs to connect to the RLC. It must be a DID number.

Data port configuration for 911x on the Meridian 1 PBX

This section shows the configuration settings for the data port on the Meridian 1 PBX. The data port provides the communication path between the RLC and the Remote Office 911x series unit, and must be configured as an ATA.

Configuration example

This configuration sample is from a Meridian 1 PBX 11.

```
REQ: prt
TYPE: 2616
MARP NOT ACTIVATED
TN   9 16
DATE
PAGE
DES
DES  NO DES
TN   009 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
SFLT NO
CAC_CIS 3
CAC_MFC 0
```

Telephone type

RLC slot and port numbers

TGAR must be configured to allow trunk access. Refer to your PBX documentation for more details.

VCE defines the port as a voice port.

```
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 SLKD CCSD SWD LND CNDD
     CFTD SFD MRD DDV CNIA CDCA MSID DAPA BFED RCBD
     ICDD CDMD LLCN MCTD CLBD AUTU
     GPUD DPUD DNDD CFXD ARHD CLTD ASCD
     CPFA CPTA HSPD ABDD DELD CFHD FICD NAID DNAA BUZZ AGRD MOAD
UDI RCC HBTD AHD IPND  DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
    USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXA FTTC DNDY DNO
MCBN
CPND_LANG ENG
HUNT
PLEV 02
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
DNDR 0
DTMK
KEY  00 SCR 9016 0     MARP
        ANIE 0
     01
     02
     03
     04
     05
     06
     07
     08
     09
     10
     11
     12
     13
     14
     15
```

The number that the Remote Office 911x series unit needs to connect to the RLC. It must be a DID number.

Voice port configuration on the CS 2100 PBX

This section shows the datafill for a typical M2616 subscriber line. Voice ports (telephones) must be datafilled on the even numbered LENs in the CS 2100 The even numbered ports correspond to ports 0-15 on both the RLC at the host site, and the Remote Office 9110, 9115, or 9150 unit(s) at the remote site(s) served by the RLC.

Configuration example

```
>table lninv
TABLE: LNINV
>add
LEN:
>host 19 1 4 0                ← This is the LEN address in the CS 2100
CARDCODE:
>DR68AA                       ← This is the card that will be occupying the IPE slot
PADGRP:
>DONS
STATUS:
>hasu                         ← HASU , meaning Hardware Assigned, Software
Unassigned
GND:
>n
BNV:
>nl
MNO:
>y
CARDTYPE:
>nil
TUPLE TO BE ADDED:
HOST  19 1 04 0   DR68AA   DONS     HASU   N  NL   Y              NIL
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y

>servord
SO:
>new
```

This is an example of a typical M2616 telephone set:

```
SONUMBER:      NOW    0   9 22 PM
>
DN:
>6846100                    ← Site Specific information, is the DN of the instrument
LCC_ACC:
>m2616                      ← Telephone Type.
RINGTYPE:
>fh
HANDS_FREE:
>y
GROUP:
>ntirich                    ← Site Specific information. This will vary between sites
SUBGRP:
>0                          ← Site Specific information. This will vary between sites
NCOS:
>64                         ← Site Specific information. This will vary between sites
SNPA:
>972                        ← Site Specific information. This will vary between sites
KEY:
>1
RINGING:
>y
LEN_OR_LTID:
>19 1 4 0                   ←This is the LEN of the Voice Port.
OPTKEY:
>1
OPTION:
>m0200                      ← This is the option for a display.
OPTKEY:
>$
COMMAND AS ENTERED:
NEW NOW 0 9 22 PM 9726100 M2616 FH Y NTIRICH 0 64 972 1 Y HOST 19 1 04
00 ( 1
M0200 ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
2000/09/22 12:34:41.571 FRI.   JOURNAL FILE RECORD ID 62
```

Data port configuration for 9150 on the CS 2100 PBX

This section shows the configuration settings for the MCA data port on the CS 2100 PBX. The data port provides the communication path between the RLC and the Remote Office 9150 unit, and must be configured as an MCA. MCAs must be datafilled on the odd numbered LENs in the CS 2100. The odd numbered ports correspond to ports 16-32 on both the RLC and the Remote Office 9150 unit.

Configuration example

```
>table lninv
TABLE: LNINV
>add
LEN:
>host 19 1 4 31              ← This is the LEN address in the CS 2100.
CARDCODE:
>DR68AA                      ← This is the card that will be occupying the IPE slot.
PADGRP:
>DONS
STATUS:
>hasu                        ← HASU , meaning Hardware Assigned, Software
Unassigned
GND:
>n
BNV:
>nl
MNO:
>y
CARDTYPE:
>nil
TUPLE TO BE ADDED:
HOST  19 1 04 31   DR68AA   DONS     HASU   N  NL   Y              NIL
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>Y

>servord
SO:
>new
SONUMBER:     NOW   0  9 21 AM
```

CS 2100 Data port configuration (cont'd.)

```
DN:
>6846789                    ← Site Specific information. This will vary between sites.
LCC_ACC:
>mca                        ← Field denotes line type.
GROUP:
>NTIRICH                    ← Site Specific information. This will vary between sites.
SUBGRP:
>0                          ← Site Specific information. This will vary between sites.
NCOS:
>64                         ← Site Specific information. This will vary between sites.
SNPA:
>972                        ← Site Specific information. This will vary between sites.
RINGING:
>y
CLASSDU:
>mca
DOWNLOAD:
>n
SYNCHRO:
>s
DATARATE:
>64000
CLOCKSRC:
>i
V25:
>n
HDLC:
>n
RTS:
>n
HOTLINE:
>n
VLL:
>n
IDLETO:
>0
KBDTYP:
>hayes
DPOPTS:
>$
LATANAME:
>nillata
```

CS 2100 Data port configuration (cont'd.)

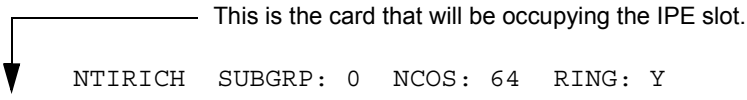
```
LEN_OR_LTID:
>19 1 4 31                    ← Site Specific information. This will vary between sites.
OPTION:
>ndc
OPTION:
>$
COMMAND AS ENTERED:
NEW NOW 0 9 21 AM 6846789 MCA NTIRICH 0 64 972 Y MCA N S 64000 I N N N
N N
0 HAYES $ NILLATA HOST 19 1 04 31 ( NDC ) $
ENTER Y TO CONFIRM,N TO REJECT OR E TO EDIT
>y
```

Data port configuration for 911x on the CS 2100 PBX

This section shows the configuration settings for the ATA data port on the CS 2100 PBX. The data port provides the communication path between the RLC and the Remote Office 911x unit, and must be configured as an ATA. ATAs must be datafilled on the odd numbered LENs in the CS 2100. The odd numbered ports correspond to ports 16-32 on both the RLC and the Remote Office 911x series unit.

Configuration example

```
TABLE: LNINV
>pos 19 1 06 03
HOST  19 1 06 03   DR68AA   DONS  WORKING   N  NL   Y
FLXA
>cha
CARDCODE: DR68AA
>
PADGRP: DONS
>
STATUS: WORKING
>
GND: N
>BNV: NL
>MNO: Y
>CARDTYPE: FLXA  <-------------- Must be FLXA for 911x network port.
>
TUPLE TO BE CHANGED:
HOST  19 1 06 03   DR68AA   DONS  WORKING   N  NL   Y
FLXA
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
LEN:     HOST  19 1 06 03 <-- This is the LEN address in the CS 2100.
TYPE: SINGLE PARTY LINE
SNPA: 972
DIRECTORY NUMBER:     6846779
LINE CLASS CODE:  M3904 WITH HANDSFREE
```




```
CUSTGRP:        NTIRICH  SUBGRP: 0  NCOS: 64  RING: Y
CARDCODE:  DR68AA    GND: N  PADGRP: DONS  BNV: NL MNO: Y
PM NODE NUMBER     :    163
PM TERMINAL NUMBER :    196
DNGRPS OPTIONS:
NETNAME: NORTEL
ADDRESS:              DDD44NNNNN
NETNAME: PUBLIC
ADDRESS:              97268NNNNN
OPTIONS:
 NONE

   KEY       DN
   ---       --
     1       DN          9726846779

   KEY     FEATURE
   ---     -------
  NONE
```

RLC configuration

This section shows the configuration settings for the RLC. You can obtain a similar configuration printout by performing a configuration download while connected to the RLC.

Note: Configuration settings are separated by commas (,).

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 351.

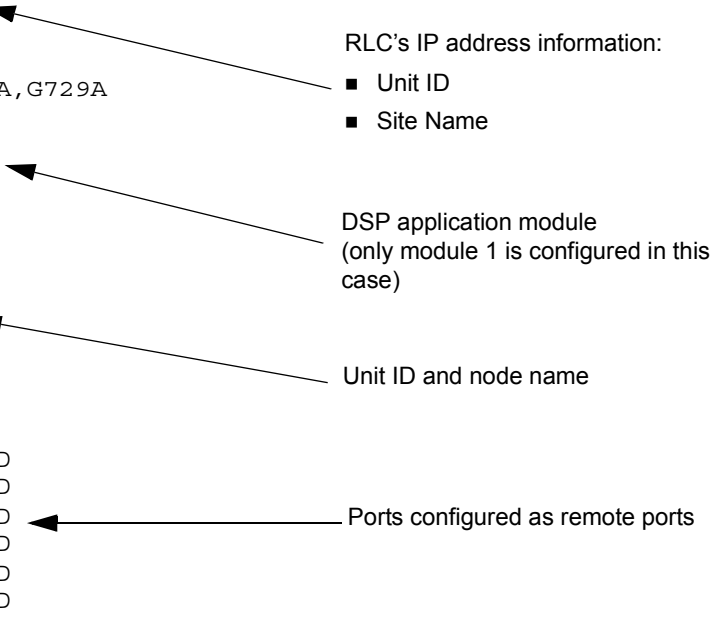
```
SYSCFG 254,HOST1

APPMODCFG 0,NC,NC
APPMODCFG 1,E,G729A,G729A
APPMODCFG 2,NC,NC
APPMODCFG 3,NC,NC

SYSCFG 254,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,5.6.7.8,
         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
```

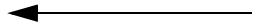
Ports configured as local ports

Port configured as network port

Remote unit connection information (unit 1):

- remote unit number
- unit ID
- security information (inbound and outbound security IDs)
- remote unit's IP address
- network port
- PSTN number

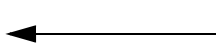
```
ONOFFCFG 1,SUN,0 00:00
ONOFFCFG 1,MON,0 00:00
ONOFFCFG 1,TUE,0 00:00
ONOFFCFG 1,WED,0 00:00
ONOFFCFG 1,THU,0 00:00
ONOFFCFG 1,FRI,0 00:00
ONOFFCFG 1,SAT,0 00:00
ONOFFCFG 2,SUN,0 00:00
ONOFFCFG 2,MON,0 00:00
ONOFFCFG 2,TUE,0 00:00
ONOFFCFG 2,WED,0 00:00
ONOFFCFG 2,THU,0 00:00
ONOFFCFG 2,FRI,0 00:00
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
```



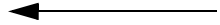
```
ONOFFCFG 6,SAT,0 00:00
ONOFFCFG 7,SUN,0 00:00
ONOFFCFG 7,MON,0 00:00
ONOFFCFG 7,TUE,0 00:00
ONOFFCFG 7,WED,0 00:00
ONOFFCFG 7,THU,0 00:00
ONOFFCFG 7,FRI,0 00:00
ONOFFCFG 7,SAT,0 00:00
ONOFFCFG 8,SUN,0 00:00
ONOFFCFG 8,MON,0 00:00
ONOFFCFG 8,TUE,0 00:00
ONOFFCFG 8,WED,0 00:00
ONOFFCFG 8,THU,0 00:00
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
```



QoS settings (these are default settings)



Caller ID (not configured; one line for each remote unit)

Remote Office 9150 unit configuration

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 351.

```
IPCFG 5.6.7.8,255.255.0.0,5.6.7.9
```

9150 unit's IP interface information:

- IP address
- Subnet mask
- IP gateway

```
APPMODCFG 0,SPARE,TSIDSP
APPMODCFG 1,E,G729A,G729A
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 254,3,0987654321,1234567890,E,1.2.3.4,E,6135551234,E,D
```

Host PBX connection information:

- RLC's unit ID
- security information (inbound and outbound security IDs)
- RLC's IP address
- 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 64,2,31,E,E,E,FAX,8664,900
```

Port (station) configuration:

- Port number
- Local and remote capability
- CPID
- DN
- Restricted digits

Unconfigured ports

Note: The default capability is Remote.

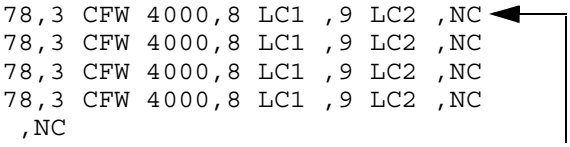
Fax port configuration:

- Port number
- Local and remote capability
- CPID
- 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)

Remote Office 911x series unit configuration

This section shows the configuration settings for the Remote Office 911x series unit. You can obtain a similar configuration printout by performing a configuration download while connected to the Remote Office 911x series unit.

Note: Configuration settings are separated by commas (,).

Configuration example

This configuration example uses the settings identified in the network diagram shown on page 351.

```
IPCFG 5.6.7.8,255.255.255.0,5.6.7.9
SYSCFG 1,Node 1
ROUCFG 0,911,#99,#98,D,#97,#96
ACCFG N
RLCDETCFG 254,0,1,E,1.2.3.4,E,6135551234
```

911x unit's IP interface information:

- IP address
- Subnet mask
- IP gateway

Unit ID and node name

System configuration:

- Emergency service number
- SPRE codes

Host PBX connection information:

- RLC's unit ID
- security information (inbound and outbound security IDs)
- RLC's IP address
- RLC PSTN number

Appendix C

Pin-out tables for RLC Multi-I/O cables

In this appendix

Reading the tables

When you read the heading, entry, heading, entry, and so on, along a single line in the tables in this appendix, the words form a complete sentence.

For example, the first line of the table below is read as follows:

In pair 1 of bundle W1, the red wire connects pin P1-21 to pin P2-5 and carries the following signal: EN0RXD+.

In pair	**of bundle**	**the**	**wire connects pin**	**to pin**	**and carries the following signal:**
1	W1,	RED	P1-21	P2-5	EN0RXD+.
1	W1,	BLK	P1-46	P2-12	EN0RXD-.
2	W1,	WHT	P1-22	P2-6	EN0TXD+.
2	W1,	BLK	P1-47	P2-13	EN0TXD-.

IF the first entry in a row is in column	THEN **the final column shows the**
four	signal carried between the named pins.
five	function of the named pin.

RLC Multi-I/O cable–Basic

One RLC Multi-I/O cable–Basic (NTDR79xx) ships with each Reach Line Card (RLC). This cable provides the following connectivity:

- P1—the switch's I/O panel
- P2—an external (user) Ethernet port
- P3—serial port to admin PC

If you lose your RLC Multi-I/O cable–Basic, contact your Nortel Networks distributor and request order number A0795280 to purchase a new one.

Pin-out information

The following table shows the pin-out of the RLC Multi-I/O cable–Basic:

In pair	of bundle	the	wire connects pin	to pin	and carries the following signal:
1	W1,	RED	P1-21	P2-5	EN0RXD+.
1	W1,	BLK	P1-46	P2-12	EN0RXD-.
2	W1,	WHT	P1-22	P2-6	EN0TXD+.
2	W1,	BLK	P1-47	P2-13	EN0TXD-.
				P2-4	GND (SHD)
1	W2,	RED	P1-17	P3-3	MMIRXD.
1	W2,	BLK	P1-42	P3-2	MMITXD.
2	W2,	WHT	P1-45	P3-5	GND.
2					
			P3-1	P3-4	MMIDTR-MMIDCD
			P3-4	P3-6	MMIDTR-MMIDSR
			P3-7	P3-8	MMIRTS-MMICTS

RLC Multi-I/O cable–Enhanced

The RLC Multi-I/O cable–Enhanced (NTDR80xx) is a 6-plug cable that provides the following connectivity:

- P1—the switch's I/O panel
- P2—an external (user) Ethernet port
- P3—a serial port to admin PC
- P4—the switch's internal Ethernet port
- P5—the cross-connect to local telephones
- P6— (for future use)

You must order this cable separately by contacting your Nortel Networks distributor and requesting order code A0795281.

Pin-out information

The following table shows the pin-out of the RLC Multi-I/O cable–Enhanced:

In pair	of bundle	the	wire connects pin	to pin	and carries the following signal:
1	W1,	BLK	P1-21	P2-5	EN0RXD+.
1	W1,	RED	P1-46	P2-12	EN0RXD-.
2	W1,	BLK	P1-22	P2-6	EN0TXD+.
2	W1,	WHT	P1-47	P2-13	EN0TXD-.
				P2-4	GND (SHD).
1	W2,	BLK	P1-17	P3-3	SDIRXD.
1	W2,	RED	P1-42	P3-2	SDITXD.
2	W2,	BLK	P1-45	P3-5	GND.
2	W2,	WHT			
			P3-1	P3-4	SDIDTR-SDIDCD.
			P3-4	P3-6	SDIDTR-SDIDSR.
			P3-7	P3-8	SDIRTS-SDICTS.
1	W3,	BLK	P1-23	P4-5	EN1RXD+.
1	W3,	RED	P1-48	P4-12	EN1RXD-.
2	W3,	BLK	P1-24	P4-6	EN1TXD+.
2	W3,	WHT	P1-49	P4-13	EN1TXD-.
1	W4,	BLK	P1-1	P5-1	TCMR00.
1	W4,	RED	P1-26	P5-26	TCMT00.

In pair	of bundle	the	wire connects pin	to pin	and carries the following signal:
2	W4,	BLK	P1-2	P5-2	TCMR01.
2	W4,	WHT	P1-27	P5-27	TCMT01.
3	W4,	BLK	P1-3	P5-3	TCMR02.
3	W4,	GRN	P1-28	P5-28	TCMT02.
4	W4,	BLK	P1-4	P5-4	TCMR03.
4	W4,	BLU	P1-29	P5-29	TCMT03.
5	W4,	BLK	P1-5	P5-5	TCMR04.
5	W4,	YEL	P1-30	P5-30	TCMT04.
6	W4,	BLK	P1-6	P5-6	TCMR05.
6	W4,	BRN	P1-31	P5-31	TCMT05.
7	W4,	BLK	P1-7	P5-7	TCMR06.
7	W4,	ORG	P1-32	P5-32	TCMT06.
8	W4,	RED	P1-8	P5-8	TCMR07.
8	W4,	WHT	P1-33	P5-33	TCMT07.
9	W4,	RED	P1-9	P5-9	TCMR08.
9	W4,	GRN	P1-34	P5-34	TCMT08.
10	W4,	RED	P1-10	P5-10	TCMR09.
10	W4,	BLU	P1-35	P5-35	TCMT09.
11	W4,	RED	P1-11	P5-11	TCMR10.
11	W4,	YEL	P1-36	P5-36	TCMT10.
12	W4,	RED	P1-12	P5-12	TCMR11.

In pair	of bundle	the	wire connects pin	to pin	and carries the following signal:
12	W4,	BRN	P1-37	P5-37	TCMT11.
13	W4,	RED	P1-13	P5-13	TCMR12.
13	W4,	ORG	P1-38	P5-38	TCMT12.
14	W4,	GRN	P1-14	P5-14	TCMR13.
14	W4,	WHT	P1-39	P5-39	TCMT13.
15	W4,	GRN	P1-15	P5-15	TCMR14.
15	W4,	BLU	P1-40	P5-40	TCMT14.
16	W4,	GRN	P1-16	P5-16	TCMR15.
16	W4,	YEL	P1-41	P5-41	TCMT15.
1	W5,	BLK	P5-9	P6-2	(reserved)
1	W5,	RED	P5-34	P6-14	(reserved)
2	W5,	BLK	P5-10	P6-3	(reserved)
2	W5,	WHT	P5-35	P6-16	(reserved)
3	W5,	BLK	P5-11	P6-4	(reserved)
3	W5,	GRN	P5-36	P6-5	(reserved)
4	W5,	BLK	P5-12	P6-20	(reserved)
4	W5,	BLU	P5-37	P6-6	(reserved)
5	W5,	BLK	P5-13	P6-8	(reserved)
5	W5,	YEL	P5-38	P6-7	(reserved)
6	W5,	BLK	P5-14	P6-17	(reserved)
6	W5,	BRN	P5-39	P6-9	(reserved)

In pair	of bundle	the	wire connects pin	to pin	and carries the following signal:
7	W5,	BLK	P5-15	P6-24	(reserved)
7	W5,	ORG	P5-40	P6-11	(reserved)
8	W5,	RED	P5-16	P6-15	(reserved)
8	W5,	WHT	P5-41	P6-12	(reserved)

Appendix D

Safety and regulatory information

In this appendix

International safety compliance

The Reach Line Card (RLC) and the Remote Office system comply with international safety regulations as listed on this page.

Underwriters Laboratory (UL)

The RLC complies with and is listed under UL 1950, Third Edition, including revisions based on the Fourth Amendment to IEC 950, Second Edition.

Canadian Standards Association (CSA)

The RLC complies with and is listed under CSA C22.2, No. 950-95.

Europe

The RLC complies with and is listed under EN60950: 1992, incorporating amendments 1, 2, 3, 4 & 11.

Australia

The RLC complies with and is listed under TS001\AS 3260.

Other Countries Deviations Assessed

Refer to Nemko Test Report # 2000 29173.

Electromagnetic compatibility

The Reach Line Card (RLC) does not interfere with operation of other licensed communications systems according to the standards set forth by Australia, the United States, and Canada.

The RLC does not adversely effect the compliance of the Meridian 1 PBX system to:

- AS 3548 Class B (Australia)
- Class A of FCC Part 15, Subpart J
- CSPR B requirements[i]

The margin is at least 2 dB better than the specified limit.

i. CSPR B limits the number of RLCs that can be used in an Meridian 1 PBX 11 cabinet with the RLC Multi-I/O cable–Enhanced to five (5).

Electromagnetic immunity

The RLC in a Meridian 1 PBX resists electromagnetic interference.

The RLC performs normally when subjected to narrow band radiated fields in frequency range 500 kHz to 1 GHz (field strength up to 10 V/m, 1 kHz, 50% modulated AM signal) per IEC 1000-4-3.

Electrostatic discharge

The Reach Line Card (RLC) is immune to electrostatic discharges typical for an office environment (carpeted floors, low humidity) according to the test method specified by IEC 1000-4-2.

No damage or malfunction occurs when the RLC is exposed to up to +/-8kV of direct discharge. An indirect discharge of up to +/-16 kV does not result in malfunction of the system (to adjacent equipment or connected cabling).

The requirements for both “closed door” and “open door” have been met.

Glossary

10BaseT Ethernet
The Ethernet standard for baseband local area networks using twisted-pair cable carrying 10 megabits per second (Mbps) in a star topology.

A

A-law
A companding technique used in encoding and decoding audio signals in 30-channel pulse code modulated (PCM) systems. A-law companding is the primary method used in Europe. *Refer also to* 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 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
Refer to 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.

Asynchronous Transfer Mode

A network technology that uses start bits and stop bits (identifying the beginning and end of digital code) to facilitate data transfer. ATM equipment can transmit video, audio, and computer data over the same network, ensuring that no single type of data dominates the line.

ATM

Refer to Asynchronous Transfer Mode.

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 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

Refer to 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.

Basic Rate Interface

An ISDN subscriber service that uses two B (64Kbps) channels and one D (64 Kbps) channel to transmit voice, video, and data signals.

BIOS
Refer to 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.

Boolean logic
A logic system that enables a computer to use electricity to make complex decisions. The basic logic gates (And, Or, and Not) determine the flow of electricity through the computer's circuitry and whether specific computing functions are carried out.

boolean
A value that can only be true or false.

branch station
A telephone set located at the Remote Office 9110, 9115, 9150, or Meridian Digital Telephone IP Adapter site.

BRI
Refer to Basic Rate Interface.

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.

bridge port
Bridge ports are configured on the Remote Office 9150 unit and are used to connect branch office trunks through the host PBX to accommodate conference calls, remote station to remote station calls, and so on.

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 PSTN 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, that 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 RLC to identify the number of the caller requesting access to one of its ports. It is also used on remote units to authenticate incoming calls from the 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 that chips and other electronic components are placed on. Examples of cards include motherboards, expansion boards, daughterboards, controller boards, network interface cards, and video adapters.

Central Processing Unit
This is the system unit that holds a PC's essential components.

CBT
Refer to Computer-Based Training.

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.

chip
The small flake of silicon crystal that makes up the microprocessor. 2. A type of controller.

CLAN
Refer to Customer Local Area Network.

CLID
Refer to 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.

COD
Refer to Call On Demand.

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
A type of education that 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 remote units and the RLC port that they are connected to.

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
Refer to Central Processing Unit.

CPU clock
The clock that regulates the execution of instructions inside a computer. *Refer also to* real-time clock.

crash
A serious computer failure whereby 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 that your corporate services and resources connect to. The 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.

DB9 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.

DC
Refer to Direct Current.

DHCP
Refer to Dynamic Host Configuration Protocol.

Digital Linear Tape
A high-capacity 1/2-inch streaming tape cartridge format.

Digital Signal Processor
A special type of coprocessor that manipulates analog data, such as sound or photographs, that has been converted to digital form.

DIMM
Refer to Dual In-line Memory Module.

DIP
A type of protective packaging for silicon memory chips that provides a safe and convenient means of installing and removing the chip.

DIP switch
A series of tiny switches built into circuit boards that enables you to configure a circuit board for a particular type of computer or application. DIP switches are always toggle switches. This means that they have two possible positions: on or off (or 1 or 0).

Direct Current

DC, the electrical power used by computers, comes from a single source (such as a battery) that provides a single voltage that stays at a constant level. AC, the power provided by utility companies, must be converted to DC before it can be used in computer systems.

Direct Memory Access

DMA speeds up system performance by moving blocks of memory around inside the computer (typically between I/O devices and memory). This process enables the microprocessor to spend its time performing other functions.

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

Refer to Dynamic Link Library.

DLT

Refer to Digital Linear Tape.

DMA

Refer to Direct Memory Access.

DN

Refer to 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

Refer to Digital Signal Processor.

Dual In-line Memory Module
The protective packaging for microprocessor chips that provides a safe and convenient means of installing and removing the chip.

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 RLC feature that is similar to multiuser ports in that multiple stations can share ports on the RLC. However, users sharing ports from a dynamic pool are assigned to the first available port on the RLC.

E

ECC
Refer to Error Correction Code.

ECP
Refer to Extended Capabilities Port.

EEPROM
Refer to Electronically Erasable Programmable Read-Only Media.

EIDE
Refer to Enhanced IDE.

EISA
Refer to Extended Industry Standard Architecture Bus.

ELAN
Refer to 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.

Electrostatic Discharge

Discharge of a static charge on a surface or body through a conductive path to ground. Can be damaging to integrated circuits.

Embedded Local Area Network

This is the network connection from the host PBX to the RLC. It is an Ethernet LAN that is segmented from the rest of the Ethernet network and enables signaling and administration access to the 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

Electro-magnetic interference. Interference in signal transmission or reception caused by the radiation of electrical and magnetic fields.

Enhanced IDE

An IDE hard disk interface enhanced with hardware and firmware changes to support disks larger than 540 Mbytes, four disks instead of two, and faster transfer rates. *Refer also to* IDE.

Enhanced Parallel Port

A parallel port standard for PCs that supports bidirectional communication between the PC and attached devices (such as a printer).

EPP

Refer to Enhanced Parallel Port.

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).

ESD
Refer to Electrostatic Discharge.

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 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. *Refer also to* bus.

expression
A building block of a script, used to test for conditions, perform calculations, or compare values within scripts. *Refer also to* logical expression, mathematical expressions, and relational expression.

Extended Capabilities Port
A parallel-port standard for PCs that supports bidirectional communication between the PC and attached devices (such as a printer).

Extended Industry Standard Architecture Bus
A 32-bit bus that accommodates ISA PC boards.

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, that 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.729A

G.729A 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.729A provides 8 Kbps 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 RLC.

Gbyte

Refer to Gigabyte.

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.

Gigabyte
1 073 741 824 bytes. One Gbyte is equal to 1024 Mbytes.

GPCP
General purpose computing platform

GPF
Refer to 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.

GUI
Refer to graphical user interface.

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 host 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 PSTN.

hub
A common connection point for all 10BaseT 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.

IDE
Commonly used to describe the AT attachment design, the dominant hard disk interface. IDE is a cost-effective interface technology for mass storage devices that the controller is integrated into the disk or CD-ROM drive in.

idle timer
Identifies the maximum length of time that 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.

Industry Standard Architecture
A 16-bit standard interface for add-in cards.

Input/Output
Refers to any operation, program, or device that enters data into a computer or extracts data from a computer.

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). *Refer also to* BRI.

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.

I/O
Refer to Input/Output.

IP
Refer to Internet Protocol.

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 could be an IP address.

IPX
Internetwork Packet Exchange. A networking protocol used by the Novell NetWare operating systems.

ISA
Refer to Industry Standard Architecture.

ISDN
Refer to Integrated Services Digital Network.

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
Refer to kilobyte.

kilobyte
1024 bytes. Roughly the amount of information in half a typewritten page.

L

LAN
Refer to Local Area Network.

LCD
Liquid crystal display. An alphanumeric display using liquid crystal sealed between two pieces of glass.

LED
Light emitting diode. A semiconductor diode that emits light when a current is passed through it.

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 site that is used to call another station at the branch office, or to place and receive calls through the local PSTN.

local station
A telephone set located at a remote site.

locally 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 locally controlled call mode. Calls in locally controlled mode are routed through the local PSTN.

logical expression
A symbol used in scripts to test for different conditions. Logical expressions are AND, OR, and NOT. *Refer also to* mathematical expressions and relational expression.

M

M1
Meridian 1 PBX

mathematical expressions
The expressions used in scripts to add, subtract, multiply, and divide values. Mathematical expressions are addition (+), subtraction (-), division (/), and multiplication (*). *Refer also to* logical expression, relational expression.

Mbyte
Refer to megabyte.

megabyte
A unit of measurement for data storage equal to 1 048 576 bytes.

megahertz
One million cycles per second.

MHz
Refer to megahertz.

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 *Refer also to* A-law.

multiuser ports

A Remote Office 9150 unit port feature that allows multiple stations to time-share a single port on the host PBX. All stations that use a multiuser port are always assigned to the same port number (TN) on the host PBX.

N

NetBeui

Refer to NetBIOS enhanced user interface.

NetBIOS

Refer to Network Basic Input Output System.

NetBIOS enhanced user interface

An enhanced version of the NetBIOS protocol used by network operating systems such as LAN Manager, LAN Server, Windows for Workgroups, Windows 95 and Windows NT.

Network Basic Input Output System

An application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities.

Network Interface Card

An expansion board that enables a PC to be connected to a local area network (LAN).

NIC

Refer to Network Interface Card.

node

A device connected to the network capable of connecting to other network devices. For example, the RLC and each remote unit are nodes on the network.

NPA

Refer to Number Plan Area.

Number Plan Area
Area code

NVRAM
Non-Volatile Random Access Memory. RAM that doesn't lose its memory when you shut the electricity off to it.

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.

ODBC
Refer to Open Database Connectivity.

OEM
Original Equipment Manufacturer. The maker of equipment marketed by another vendor, usually under the name of the reseller. The OEM may only manufacture certain components, or complete computers, that are then often configured with software and/or other hardware, by the reseller.

OLE
Refer to Object Linking And Embedding.

online/offline table
The online/offline table is configured on the RLC. It allows you to schedule times that the host PBX connection is made available to the remote site and the 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 Database Connectivity
A Microsoft-defined database Application Program Interface (API) standard.

Open System Interconnection
A worldwide communications standard that defines a framework for implementing protocols in seven layers.

OS
Operating Standard

OSI
Refer to Open System Interconnection.

OTM
Optivity Telephony Manager. This is a Nortel Networks software application that is used to administer the Meridian 1 PBX.

P

Packet InterNet Groper
PING. A protocol that can be used to test the Ethernet connection to devices on the network (such as the RLC and its associated remote units).

packetized voice
Digital signal processors (DSPs), located in the Remote Office 9150 unit and 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.

parallel port
A type of interface used to connect an external device such as a printer to a PC. Most personal computers have both a parallel port and at least one serial port.

PBX
Refer to Private Branch Exchange.

PC
Personal computer. A computer with an architecture that is compatible with the IBM PC.

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 that an agent can be reached directly on, usually for private calls.

phoneset
The physical device, connected to the switch, calls are presented to.

PING
Refer to Packet InterNet Groper.

position ID
A unique identifier for a phoneset, used by the switch to route calls to the phoneset.

POST
Refer to 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 placing telephone calls external to the PBX.

protocol

A standard format used for communication between two devices. The protocol determines the type of error checking to be used, the data compression method (if any), how the sending device will indicate that it has finished sending a message, and how the receiving device will indicate that it has received a message.

PSTN

Refer to Public Switched Telephone Network.

Public Switched Telephone Network

Any common carrier network that provides circuit switching between public users. The term is usually applied to the public telephone network.

Q

Quality of Service (QoS) Transitioning Technology

Nortel Networks' patented technology that can automatically switch calls from the IP network to the PSTN when the voice QoS falls below a predetermined threshold, and back to the IP network when the QoS 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.

RAS

Remote Access Server. A host on the local area network that is equipped with modems to enable users to connect to the network over telephone lines.

real-time clock
A clock that keeps track of the time even when the computer is turned off. *Refer also to* CPU clock.

recorded announcement route
A resource installed on the switch that offers a recorded announcement to callers.

relational expression
An expression used in scripts to test for different conditions. Relational expressions are less than (<), greater than (>), less than or equal (< =), greater than or equal (> =), and not equal (< >). *Refer also to* logical expression and mathematical expressions.

Remote Access Services
A feature built into Windows NT and Windows 95 that enables users to log in to an NT-based LAN using a modem, X.25 connection, or WAN link. Also known as Dial Up Networking.

remote station
A telephone set located at the Remote Office 9110, 9115, 9150, or Meridian Digital Telephone IP Adapter site.

remote trunk
From the RLC's point of view, remote trunks are the ISDN BRI connections between the PSTN and the remote unit located at the branch office site.

RJ-11 Connector
A six-conductor modular jack that is typically wired for four conductors. The RJ-11 jack is the most common telephone jack in the entire world.

RJ-45 Connector
An eight position, eight conductor modular jack used for data transmission over a standard telephone wire. The RJ-45 jack provides the 10BaseT Ethernet connection.

RLC
An abbreviation for Reach Line Card. The RLC is installed on the host PBX and relays voice and signaling information from the digital telephones connected at a remote site to the host PBX.

ROM
Read-Only Memory. This is the computer memory that data has been prerecorded on and cannot be removed from.

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.

RTC
Refer to real-time clock.

S

SCA
Refer to Single Connector Architecture.

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 RLC for each connection request. The RLC matches the identifier configured for the RLC port. When it finds a match, it grants access to the port and allows the call to proceed.

Sequenced Packet Exchange
A transport layer protocol (layer 4 of the OSI Model) used in Novell Netware networks. The SPX layer sits on top of the IPX layer (layer 3) and provides connection-oriented services between two nodes on the network. SPX is used primarily by client/server applications.

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.

Service Profile Identifier
When you order an ISDN line, your phone company provides you with a SPID for every phone number you have.

silence suppression
A feature that prevents packet transmission during periods when there is no voice data present.

SIMM
Single In-line Memory Module. Used on Macs and PCs. A form of chip packaging where leads (pins) are arranged in a single row protruding from the chip.

Simple Network Management Protocol
A set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network and then analyzing the responses.

Single Connector Architecture

A method for supplying power and data lines in one connector on hard disks. Provides hot-swap capability.

single-user ports

A RLC port that supports one remote station.

Small Computer System Interface

A standard for connecting and controlling mass storage devices such as CD-ROMS, tape drives, and hard disks.

SNMP

Refer to Simple Network Management Protocol.

SPID

Refer to Service Profile Identifier.

SPRE code

A Special Prefix code that is used to initiate use of a host 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 locally controlled mode so that local calls can be made
- register a Remote Office 9150 unit for a multiuser or dynamic port

SPX

Refer to Sequenced Packet Exchange.

SRAM

Static Random Access Memory. A form of RAM that retains its data without the constant refreshing that DRAM requires.

station

A telephone or fax machine located at a remote 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 RLC or remote unit what portion of the IP address represents the network (and subnetwork) and what portion represents the host.

SVGA
Super Video Graphics Adapter. An extension of the VGA video standard.

switch
In a telecommunications network, a switch is the hardware that receives phone calls and provides connections to telephone sets. The switch allows a connection to be established as necessary and terminated when there is no longer a session to support it.

In networks, a device that filters and forwards packets between LAN segments. Switches operate at the data link layer (layer 2) of the OSI Reference Model and therefore support any packet protocol. LANs that use switches to join segments are called switched LANs or, in the case of Ethernet networks, switched Ethernet LANs.

switch resource
A device that is configured on the switch.

T

TAPI
Refer to Telephone Application Programming Interface.

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.

Telephone Application Programming Interface

A term that refers to the Windows Telephony API. TAPI is a changing (i.e. improving) set of functions supported by Windows that allow Windows applications to program telephone-line based devices such as single and multi-line phones (both digital and analog), modems and fax machines in a device-independent manner.

telephony

The science of translating sound into electrical signals, transmitting them, and then converting them back to sound. The term is used frequently to refer to computer hardware and software that perform functions traditionally performed by telephone equipment.

TFTP

Refer to Trivial File Transfer Protocol.

threshold

A value for a statistic that system handling of the statistic changes at.

threshold class

A set of options that specifies how statistics are treated in reports and real-time displays. *Refer also to* pegging threshold.

Token Ring

A PC network protocol developed by IBM. A Token Ring network is a type of computer network whereby all the computers are arranged schematically in a circle.

Trivial File Transfer Protocol

A simplified version of FTP that transfers files but does not provide password protection or user-directory capability. It is associated with the TCP/IP family of protocols. TFTP depends on the connectionless datagram delivery service, UDP.

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 digits

Trunk access digits are numbers that are used by the remote unit to determine the trunk to use when routing a call. For example, 9 is a common trunk access digit used to obtain an outside line.

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 PSTN. 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 locally 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

Refer to 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

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 Internet Protocol (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

Symbols

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Reach Line Card
Installation and Administration Guide

Printed in Canada.

Publication number:	555-8421-210
Product release:	1.5
Document release:	Standard 3.0
Date:	July 2004