555-8321-310

Meridian HomeOffice II

Network Administration Guide

Product release 2.1   Standard 01.02   July 1999

NORTEL NETWORKS™

How the world shares ideas.

Meridian HomeOffice II

Network Administration Guide

Publication number:	555-8321-310
Product release:	2.1
Document release:	Standard 01.02
Date:	July 1999

Printed in Canada

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

Publication history

July 1999

This is the Standard 01.02 issue of the *Network Administration Guide* for Product release 2.1 of Meridian HomeOffice II. This guide has been rewritten to make it more usable for network administrators.

July 1998

This is the Standard 01.01 issue of the *Network Administration Guide* for Product release 2.1 of Meridian HomeOffice II. Written for the network administrator at the corporate host site, it explains how to configure the HomeOffice Router for operation on the network. This guide includes configuring the HomeOffice Router for interoperability with Rapport devices such as Dialup Switches.

Contents

2 Preparing for implementation 69

3 Configuring the HomeOffice Router 83

Section A: Using Local Manager 93

Section B: Configuring the ISDN interface and circuits 101

Section C: Data circuit configuration reference 139

Preface

About this document

In this preface

Overview

Introduction

This document explains how to configure the HomeOffice Router for operation on the network from a network administrator's point of view.

Who should read this guide

This guide is written for HomeOffice II data network managers and administrators at the corporate host site.

Assumptions

This guide assume that you are familiar with the following:

- data networking concepts and operation
- Windows PCs
- remote access switches

Version and issue of HomeOffice II documentation

The version and issue of Meridian HomeOffice II documents are indicated by a four-digit document release number (for example, 01.01). The first two digits indicate the version, or release of the product. The second two digits indicate the issue of the documentation.

The first two digits increase by one each time the document content is changed to support a new HomeOffice II release. For example, the first release of a document is 01.01, and the next release of the document in a subsequent HomeOffice II release is 02.01. The second two digits increase by one each time a final document is revised and rereleased for the same HomeOffice II release.

HomeOffice II documentation release 01.02 is assigned to the second issue of this guide to support HomeOffice II Release 2.1.

About this guide

Introduction

This *Network Administration Guide* provides the following:

- an overview of how the HomeOffice Router fits into your data network
- the issues that you must consider
- configuration and administration instructions

How to use this guide

It is recommended that you use this guide as follows:

1. Read the following chapters to learn about the HomeOffice Router and the issues you must consider:

   — Chapter 1, “Meridian HomeOffice II interoperability in a data network”

   — Chapter 2, “Preparing for implementation”
2. For detailed instructions on when to use specific features and how to configure them, refer to Chapter 3, “Configuring the HomeOffice Router.”
3. Once HomeOffice Routers have been deployed, refer to the following chapters (as required) for instructions on how to perform daily administration tasks:

   — Chapter 4, “Administration”

   — Chapter 5, “Troubleshooting network problems”

In this guide

This guide is organized into the following chapters:

Chapter 1, “Meridian HomeOffice II interoperability in a data network”
This chapter provides

- a description of the features provided by the HomeOffice Router

- an overview of what you must consider when planning to incorporate the HomeOffice Router into your data network
- diagrams of commonly used connection scenarios

Chapter 2, "Preparing for implementation"
This chapter provides

- an overview of how to incorporate Meridian HomeOffice II into your data network
- checklists and data entry forms to assist you

Chapter 3, "Configuring the HomeOffice Router"
This chapter explains how to use Local Manager to configure the HomeOffice Router. It also provides configuration instructions for features such as callback, aggregation, Dynamic IP (or IPX) Address Translation, static routes, and DNS resolution.

Chapter 4, "Administration"
Once you have completed HomeOffice Router deployment, you must maintain the network. This chapter provides a description of some suggested administration activities.

Chapter 5, "Troubleshooting network problems"
This chapter provides an overview what you can check if telecommuters are having problems with their Meridian HomeOffice II system.

Appendix A, "Recommended reading"
This appendix lists books and Internet web sites that provide more information about the following:

- networking
- ISDN
- remote access

Appendix B, "Configuration forms"
This appendix provides samples of forms that you can use to plan the configuration of telecommuters' HomeOffice Routers.

G lossary

This list provides definitions for many networking and telecommunications terms.

Indexes

The Fields index helps you to locate information about the fields on the Local Manager screens. Use the Fields index when you want to know “What does this field do?”

The main Index provides an alternative method for locating information in this guide.

Skills you need

Introduction

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

Nortel Networks product knowledge

Knowledge of, or experience with, the following Nortel Networks products will assist you when you install and use HomeOffice II:

- the HomeOffice Router
- other Nortel Networks routers
- Nortel Networks remote access switches

PC experience or knowledge

Knowledge of, or experience with Microsoft Windows 3.1, Windows 95, or Windows NT will assist you when you administer the HomeOffice Router.

Telecommunications knowledge

You should have a basic understanding of telecommunications using ISDN. Each telecommuter's home office requires ISDN BRI service to connect to the corporate PBX and data network.

Data networking knowledge

Knowledge of, or experience with the following products and principles will assist you when you install and administer HomeOffice II:

- data networking products such as

  — remote access switches

  — routers

  — bridges

- data networking principals such as
  - — network, subnet, and host addressing
  - — routing over TCP/IP or IPX
  - — security authentication
- knowledge about how your data network is set up (structure, addresses, and so on)

Other experience or knowledge

Other types of experience or knowledge that may be of use include the following:

- troubleshooting skills
- analytical skills
- ability to interpret network analyzer traces

Related documents

Introduction

This topic identifies the documents that are available for

- network administrators
- Meridian 1 or SL-100 technicians
- telecommuters

Obtaining the documents

You can order printed versions of the documents from Nortel Networks.

You can download soft copy versions (in Adobe Acrobat PDF format) from the Nortel Networks web site at http://www.nortelnetworks.com/homeoffice. When you reach this site, click Software and Documentation Distribution Center, and then download the files that you need.

Network administrator documents

***Meridian HomeOffice II Planning Guide* (NTP 555-8321-101)**
This document, written for both the telecommunications network and data network administrators, explains what you need to incorporate Meridian HomeOffice II into the corporate network. It also provides installation checklists and data entry forms.

***Meridian HomeOffice II Release Notes* (NTP 555-8321-102)**
The *Release Notes* describe the features and known problems for Meridian HomeOffice II.

The HomeOffice Router package includes a condensed version of the *Release Notes*. The Meridian HomeOffice II CD-ROM provides a version containing more detailed information.

Note: The printed copy may supersede the copy provided on the CD-ROM. You can obtain the most up-to-date version from the Nortel Networks web site.

Meridian HomeOffice II Network Administration Guide
(NTP 555-8321-310)
This document, written for the corporate data network administrator, describes data networking concepts and features, and explains how to configure the HomeOffice Router for operation within the data network.

Meridian HomeOffice II Command Shell User Guide
(NTP 555-8321-910)
This document, written for data network administrators and advanced users, explains how to use the command shell to configure the HomeOffice Router.

This document is available on the HomeOffice II CD-ROM and the Nortel Networks web site only. It is unavailable in printed format.

Meridian 1 or SL-100 installer/administrator documents

Meridian HomeOffice II Line Card Configuration Guide
(NTP 555-8321-210)
This document, written for the Meridian 1 or SL-100 installer or administrator, explains how to install and configure the HomeOffice II Line Card on the Meridian 1 or SL-100 PBX.

Meridian HomeOffice II Line Card Installer’s Notes
The *Installer’s Notes* is a quick reference document that is provided inside the HomeOffice II Line Card package. This document summarizes the installation and configuration procedures and provides cross references to other documents for more detailed information.

Note: You cannot order this document separately.

Telecommuter documents

***Meridian HomeOffice II User Guide* (NTP 555-8321-205)**
This document, written primarily for the telecommuter, explains how to install and configure the HomeOffice Router and digital telephone. It includes the information you need to configure the HomeOffice Router for operation on the corporate networks.

This document is included inside the HomeOffice Router package.

***Meridian HomeOffice II Quick Start Guide* (NTP 555-8321-900)**
This document is provided with the HomeOffice II CD-ROM, which is provided inside the HomeOffice II package. It explains what is on the CD-ROM, and provides a quick reference installation procedure.

Chapter 1

Meridian HomeOffice II interoperability in a data network

In this chapter

Overview

Introduction

This chapter provides an overview of what you need to consider when planning to incorporate the HomeOffice Router into your data network.

Interoperability issues

You need to consider the following issues when you incorporate the HomeOffice Router into your network:

- Will your remote access switch be able to support the needs of telecommuting users?
- Will your remote access switch be able to support an increase in the number of telecommuting users?
- Does your network use the TCP/IP or IPX/SPX network protocols or both?
- Does your remote access switch support both of these protocols, or just one of them?
- Does your remote access switch support the features provided by the HomeOffice Router?
- Can you provide ISDN BRI to HomeOffice Router users at your corporate host site?

HomeOffice Router connection scenarios

Before you can incorporate the HomeOffice Router into your network, you must think about its place in the network. This chapter provides an overview of three commonly used connection scenarios.

Section A: Supported networking features

In this section

Overview

Introduction

This section provides an overview of some of the HomeOffice Router features.

DIAT for IP or IPX

Dynamic IP or IPX Address Translation (DIAT for IP or IPX) on the HomeOffice Router makes a group of LAN users appear as if they are originating from one IP or IPX address. This means that no matter how many devices are connected to a LAN, the central site only needs to use a single IP or IPX address to communicate with these devices.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a TCP/IP protocol that allows the principal parameters of network devices (including IP addresses) to be assigned by central DHCP servers.

RIP and SAP

The HomeOffice Router uses Routing Information Protocol (RIP) over IP, and RIP and Service Advertising Protocol (SAP) over IPX to exchange routing and service information with other routers, and to update the information in its Routing Table.

Multiple static routes

Multiple Static Routes is a cost-saving feature that avoids running RIP over WAN links.The Multiple Static Routes feature applies only to IP and IPX traffic, allowing you to configure a maximum of three static routes to the same network from a HomeOffice Router.

Multihoming

Multihoming allows the HomeOffice Router to run more than one logical network out of a single physical network. Multihoming means that any LAN or WAN interface can have more than one logical IP network assigned to it.

This feature is available on both the Ethernet and ISDN interfaces. The total number of IP addresses on the HomeOffice Router unit must not exceed 10 (shared between the Ethernet and ISDN interfaces).

Filtering

Filtering is the process of testing whether a packet needs to be passed onto another network segment. It is designed to decrease the level of traffic on your network and is cost-effective because it eliminates most unnecessary traffic between networks.

Spoofing

Spoofing is the process by which the HomeOffice Router prevents meaningless traffic from keeping the network connection open. The settings in the HomeOffice Router's Ethernet interface control some kinds of IP spoofing that the HomeOffice Router performs. This lets you determine, for some kinds of network traffic, whether the packets are meaningful.

Aggregation

The HomeOffice Router allows the ISDN interface to temporarily provide additional bandwidth by using more virtual circuits when available. It allows you to do the following:

- Set up two or more ISDN B-channels to provide more bandwidth.

  This is known as aggregation and is done using PPP Multilink.
- Set thresholds for increasing bandwidth.

  These thresholds determine when additional virtual circuits are opened.

PPP Multilink Protocol

The PPP Multilink Protocol (RFC 1717) is a standardized extension of the Point-to-Point Protocol (PPP) standard. It allows you to

- combine channels into a multilink bundle so that data can be sent at higher rates
- use packet sequencing to order packets
- ensure compatibility between manufacturers of internetworking equipment

Security authentication

The HomeOffice Router supports three types of password authentication:

- Password Authentication Protocol (PAP)
- Challenge-Handshake Authentication Protocol (CHAP)
- Shiva Password Authentication Protocol (SPAP)

To add an extra level of security, you can use Caller ID or Calling Line Identification (CLI) to identify incoming calls. The Router stores *ISDN Address received* entries in its circuit table and checks incoming calls against these addresses.

Dynamic IP Address Translation

Introduction

This topic provides an overview of Dynamic IP Address Translation (DIAT for IP). DIAT for IP consists of two elements:

- dynamic IP address assignment
- address translation

Using DIAT for IP on the HomeOffice Router makes a group of LAN users appear as if they are originating from one IP address. This means that no matter how many devices are connected to a LAN, the central site only needs to use a single IP address to communicate with these devices.

The HomeOffice Router obtains this IP address from the central site using Dynamic IP Address Assignment. The HomeOffice Router then uses Address Translation to convert the true IP addresses of its network devices to the dynamic IP address. It uses the dynamic IP address to communicate with the central site. Both of these procedures are invisible to the Router's network.

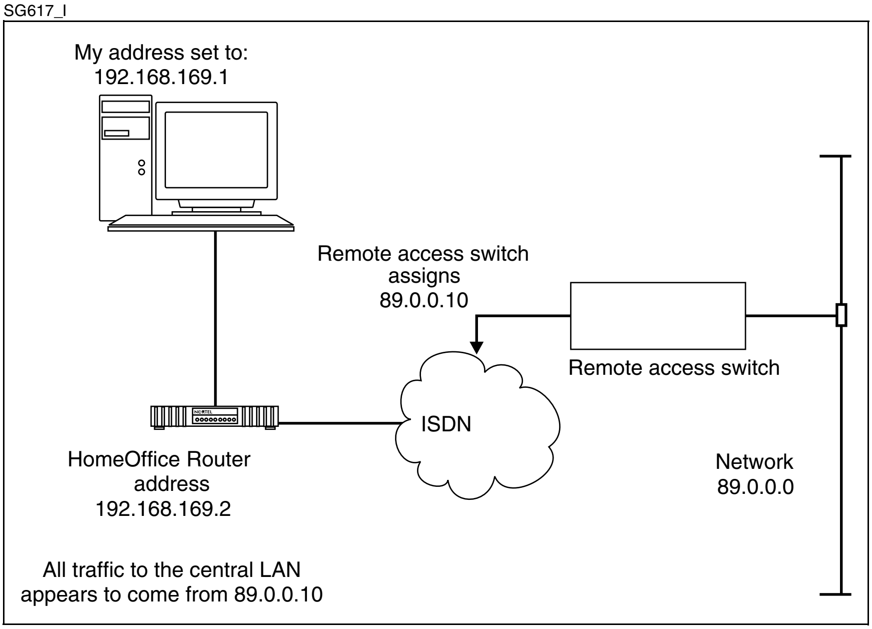
DIAT for IP benefits

DIAT for IP provides the following benefits:

- reduces the cost of Internet access
- permits access to multiple remote users at a single remote site
- conserves valuable IP address space
- provides security for remote users

How DIAT for IP works

The following illustration shows an example of how DIAT for IP works.



The HomeOffice Router ships with a default IP address, which you can use when using DIAT for IP.

The PC is configured with an address on the same LAN as the HomeOffice Router. In this example, the PC's address is 192.168.169.1. When the user starts an application that requires a network connection, the HomeOffice Router calls the central site and receives a dynamically assigned IP address. In this example, the address is 89.0.0.10.

The HomeOffice Router then translates the PC's address to the dynamically assigned IP address. Note that you never see the PC's own address outside of its own LAN.

Single-user DIAT for IP

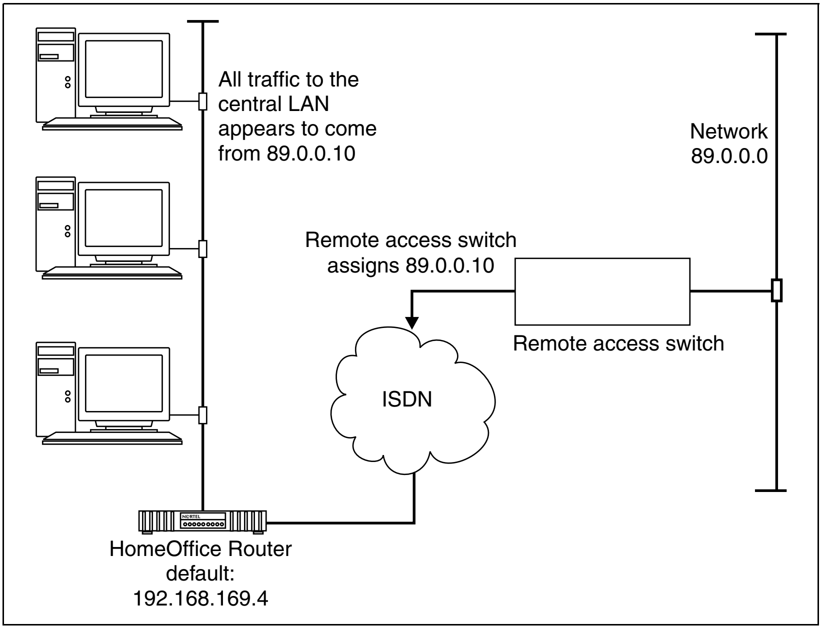
Single-user DIAT for IP simplifies the configuration of the HomeOffice Router for users who regularly access a network from different locations. For example, a user with a portable computer can access the corporate network with the same configuration as that used to connect the home office to the corporate network.

In the previous illustration, the HomeOffice Router communicates with the LAN on the 192.168.169.0 network, but communicates with the remote site over the WAN using the 89.0.0.10 address that has been invisibly assigned to it by the remote access switch.

Multi-user DIAT for IP

Use multi-user DIAT for IP when there is more than one user on the remote LAN. With multi-user DIAT for IP, the HomeOffice Router provides TCP Port Translation (as well as IP Address Translation). This ensures that packets are returned to the correct user. The remote LAN still appears as a single user to the central site.

ISG611_I


All traffic to the central LAN appears to come from 89.0.0.10
Network 89.0.0.0
Remote access switch assigns 89.0.0.10
Remote access switch
ISDN
NORTEL
HomeOffice Router default: 192.168.169.4

A key advantage of multi-user DIAT for IP is that all the remote sites can be given the same configuration by a network manager.

A disadvantage of multi-user DIAT for IP is that if a UDP port-specific application is being used, only one user can use that UDP port at any given time. This is a limitation of IP.

Using DIAT for IP with IP forwarding

There are two situations in which DIAT for IP with IP forwarding can be useful. First, it allows a user to have a single IP address configuration for the PC at home and in the office. Second, it allows a network manager to maintain and support only one boot option.

When using single-user DIAT for IP, you can use a single PC with any IP address to gain network connectivity. IP Forwarding is used in conjunction with DIAT for IP so that the HomeOffice Router can forward the PC's requests. With DIAT for IP and IP Forwarding enabled you have the same configuration at home as the one used in the office. See the illustration on the next page.

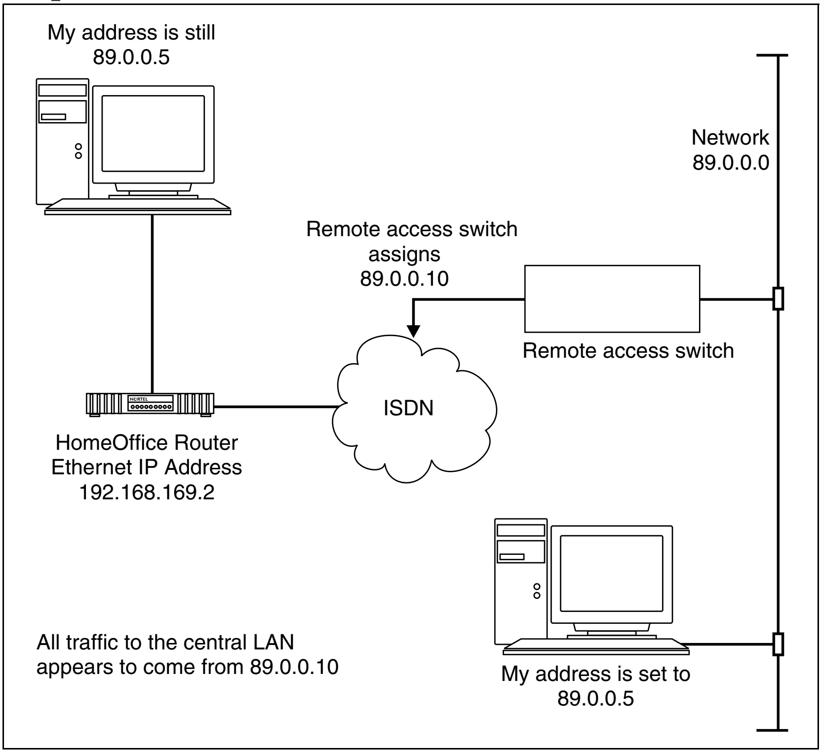
CAUTION

Risk of lost network connectivity

You can only use IP Forwarding when using DIAT for IP and when a single PC is connected by Ethernet to the HomeOffice Router.

Note: If you are using IP Forwarding, you cannot use the configuration backup, configuration restore, and upgrade functions in Local Manager from the PC connected by Ethernet to the HomeOffice Router. However, you can perform these functions by accessing HomeOffice Router remotely over an ISDN connection.

ISG614_I



By using IP forwarding, the user with an IP address of 89.0.0.5 at the central site can take the PC home and use it there without changing the IP address. The HomeOffice Router accepts packets from the PC connected to its LAN, and forwards these onto the central LAN using address translation. The HomeOffice Router also proxies ARP and acts as the default router, regardless of what address the default router is configured as on the PC.

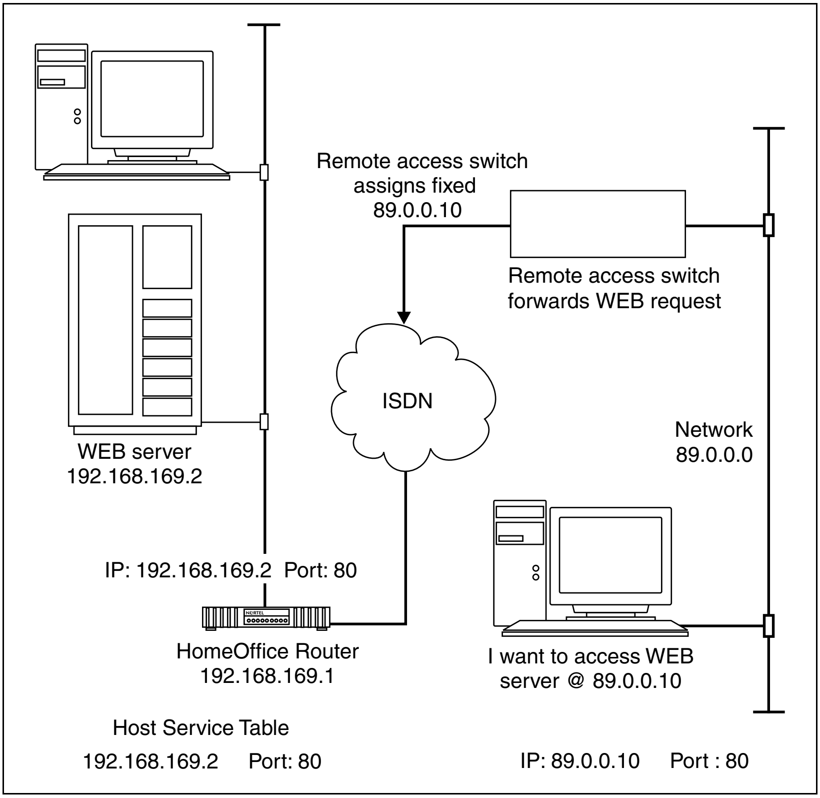
Note: This only works for single-user DIAT for IP.

DIAT for IP table

The HomeOffice Router provides a DIAT for IP table (sometimes called a host service table). This table allows applications and users at the central site to connect to services on the HomeOffice Router LAN. These services can be web services, mail services, and so on.

The HomeOffice Router is configured with a table of local services and the local address of the device supporting these services. For example, when a web request is sent to the LAN, the HomeOffice Router can forward this request to the correct device on the LAN. This allows local services to be available without the remote site having to know the local IP address.

ISG602_I


Remote access switch assigns fixed 89.0.0.10
Remote access switch forwards WEB request
ISDN
Network 89.0.0.0
WEB server 192.168.169.2
IP: 192.168.169.2 Port: 80
HomeOffice Router 192.168.169.1
I want to access WEB server @ 89.0.0.10
Host Service Table
192.168.169.2 Port: 80
IP: 89.0.0.10 Port : 80

In the preceding illustrated example of how the DIAT for IP table works, a virtual connection is set up between the HomeOffice Router and the remote access switch at the central site. This enables the remote access switch to forward packets to the remote HomeOffice Router LAN.

A DIAT for IP table is configured on the HomeOffice Router. It includes the IP address of the web server on the HomeOffice Router LAN (192.168.169.2) and the TCP port number for web servers (80). The port number defines the application.

The remote access switch assigns 89.0.0.10 as the IP address of the HomeOffice Router.

When users on the Internet or the remote access switch’s LAN want to access the web server on the HomeOffice Router LAN, they must send a packet with an IP address of 89.0.0.10 and a TCP Port number of 80.

When the HomeOffice Router receives the packet, it looks in its DIAT for IP table for an entry with Port Number 80. When it finds IP address 192.168.169.2, it changes the destination IP address of the packet and forwards the request to the web server, which then receives the packet.

Dynamic IPX Address Translation

Introduction

This section gives an overview of Dynamic IPX Address Translation (DIAT for IPX). DIAT for IPX consists of two elements:

- dynamic IPX address assignment
- address translation

When you use DIAT for IPX on the HomeOffice Router, it makes a group of LAN users appear as if it is originating from one IPX node. Use DIAT for IPX if you want IPX with DIAT for IP. This means that no matter how many devices you have connected to your LAN, the central site only needs to use a single IPX node and network number to communicate with these devices.

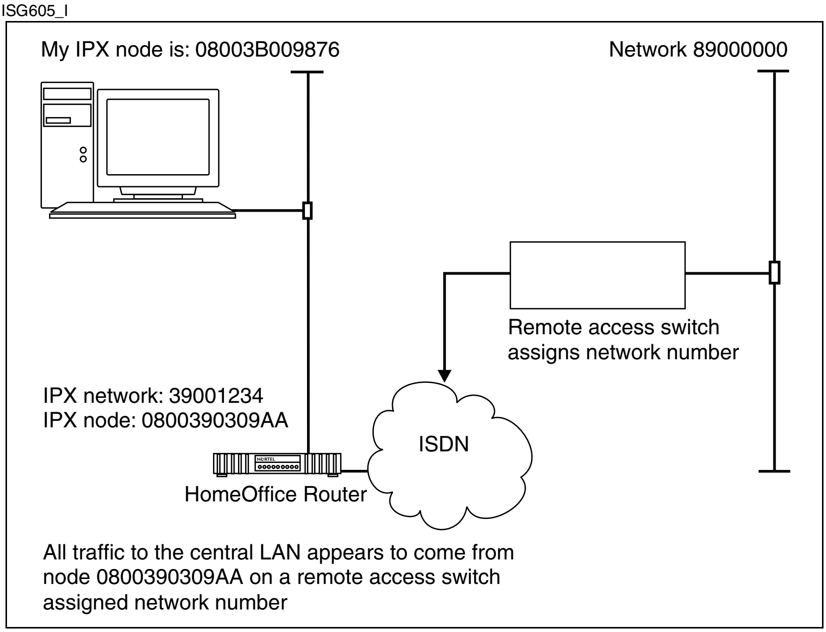
The HomeOffice Router uses its own configured IPX node number and obtains the IPX network number from the central site using dynamic IPX address assignment. The HomeOffice Router then uses address translation to convert the true IPX addresses of its network devices to the dynamic IPX address. It uses the dynamic IPX address to communicate with the central site. Both of these procedures are invisible to the Router's network.

DIAT for IPX benefits

DIAT for IPX

- eliminates the IPX routes to remote LANs, reducing central routing tables
- avoids the use of RIP and SAP, resulting in fewer ISDN calls
- allows the use of a large number of services from the remote site
- simplifies HomeOffice Router deployment
- provides security for remote users

How DIAT for IPX works


ISG605_I
My IPX node is: 08003B009876
Network 89000000
Remote access switch assigns network number
IPX network: 39001234
IPX node: 0800390309AA
ISDN
HomeOffice Router
All traffic to the central LAN appears to come from node 0800390309AA on a remote access switch assigned network number

The HomeOffice Router ships with a default IPX node number, which you can use when using DIAT for IPX.

The PC is configured with an address on the same LAN as the HomeOffice Router. In this example, the PC's network number (IPX network) is 39001234. When the user calls up an application that requires a network connection, the HomeOffice Router calls the central site and receives a dynamically assigned IPX network number.

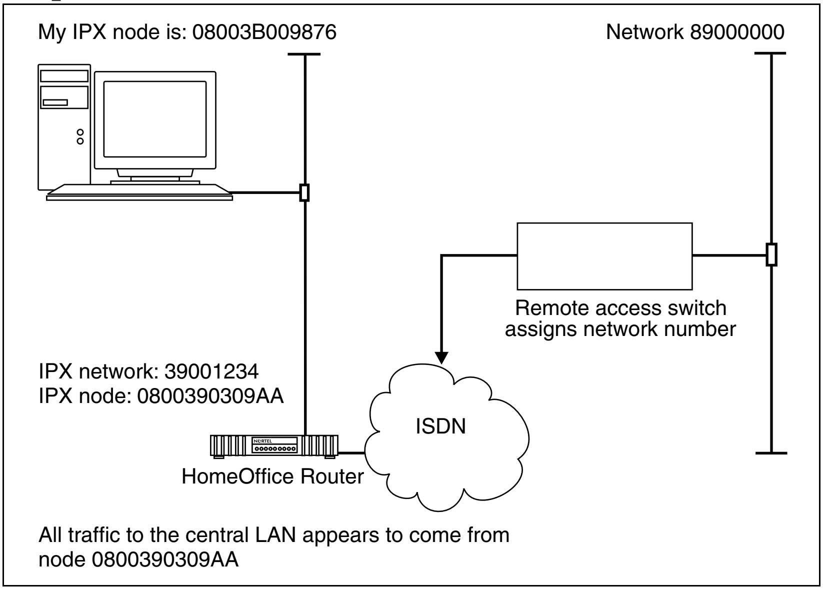
The HomeOffice Router then translates the PC's address to the dynamically assigned IPX address. Note that you never see the PC's own address outside of its own LAN.

Single-user DIAT for IPX

Single-user DIAT for IPX simplifies the configuration of the HomeOffice Router for users who regularly access a network from different locations. For example, a user with a portable computer can access the corporate network with the same configuration as that used to connect the home office to the corporate headquarters.

The following illustration shows how a user with a single PC is connected to the local network.

ISG631_I


My IPX node is: 08003B009876
Network 89000000
Remote access switch assigns network number
IPX network: 39001234
IPX node: 0800390309AA
ISDN
HomeOffice Router
All traffic to the central LAN appears to come from node 0800390309AA

The HomeOffice Router is given a default network number by the central remote access switch. It uses this network number to communicate with the central site.

However, when the HomeOffice Router communicates with the local network, a different IPX network address is used. The HomeOffice Router's Ethernet interface and the device (in this case, the user's PC) have addresses on that network.

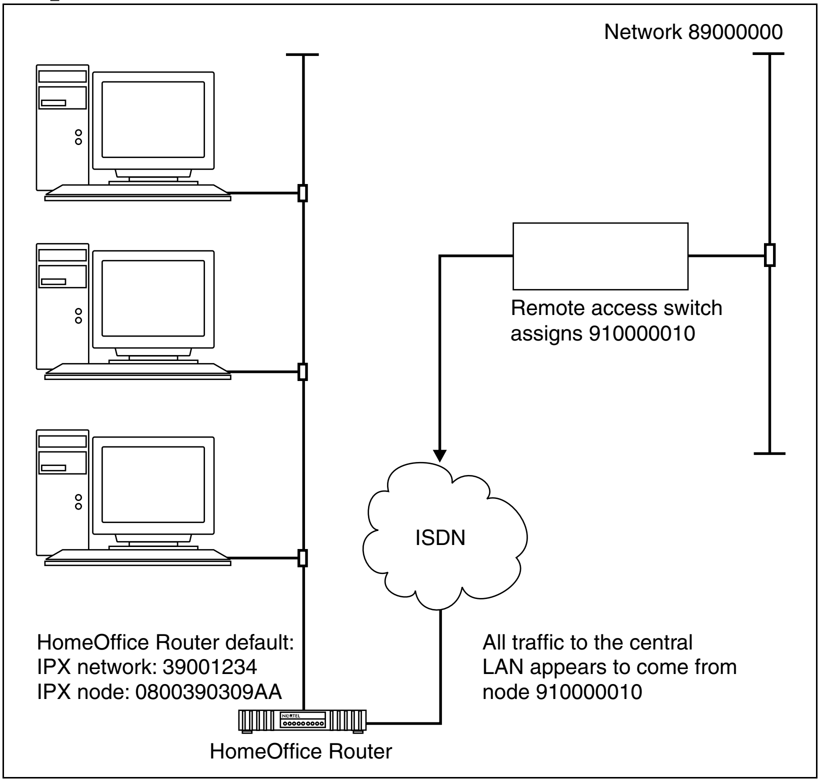
Therefore, in this example, the HomeOffice Router communicates with the LAN on the 39001234 network, but communicates with the remote site over the WAN using the address that has been invisibly assigned to it by the remote access switch.

Multi-user DIAT for IPX

Use multi-user DIAT for IPX when there is more than one user on the remote LAN. With multi-user DIAT for IPX, the HomeOffice Router provides IPX Socket Translation (as well as IPX Address Translation). This ensures that packets are returned to the correct user. The remote LAN still appears as a single user to the central site. See the following illustration.

A key advantage of multi-user DIAT for IPX is that all the remote sites can be given the same configuration at one time by a network manager.

ISG610_I


Network 89000000
Remote access switch assigns 910000010
ISDN
HomeOffice Router default:
IPX network: 39001234
IPX node: 0800390309AA
All traffic to the central LAN appears to come from node 910000010
HomeOffice Router

Dynamic Host Configuration Protocol

Introduction

Dynamic Host Configuration Protocol (DHCP) is a TCP/IP protocol that allows the principal parameters of network devices (including IP addresses) to be assigned by central DHCP servers.

Using DHCP with DIAT for IP

DHCP provides network devices with automatic configurations. When using DIAT for IP, the HomeOffice Router acts as a local DHCP server. When using DHCP, the HomeOffice Router can assign an IP address, gateway address, DNS addresses, or WINS addresses to up to 16 hosts on its Ethernet LAN.

The HomeOffice Router only acts as a local DHCP server when DIAT for IP is enabled. It is unnecessary to configure the HomeOffice Router with a pool of IP addresses as it generates addresses automatically based on its own Ethernet IP address.

Using DHCP with LAN-to-LAN connections

To enable DHCP on the HomeOffice Router when using a LAN-to-LAN connection, you must enable DIAT for IP on a circuit that is not being used. For example, if you are not using the administration circuit, you can configure it for DIAT for IP.

RIP and SAP

Introduction

The HomeOffice Router uses Routing Information Protocol (RIP) over IP, and RIP and Service Advertising Protocol (SAP) over IPX to exchange routing and service information with other routers, and to update the information in its Routing Table.

There are three ways that you can use RIP and SAP over Wide Area Networks. Each is best suited to a particular type of network:

- disabled
- broadcast (or standard) mode
- triggered mode

Disabled RIP and SAP

When RIP and SAP are disabled, routers at both sides of the WAN must be statically configured with the information that they would otherwise receive across the WAN in broadcast RIP or SAP messages. It is recommended that you use static routes or services on low bandwidth (less than 64 Kbps) lines or in cases where you cannot use Triggered RIP and SAP.

Standard RIP and SAP

When RIP and SAP operate in the standard way, messages are sent regularly (every 60 seconds for IPX and every 30 seconds for IP). This uses WAN bandwidth and causes expensive unnecessary calls on wide area networks. This mode of operation is only recommended for high bandwidth leased lines.

Note: The HomeOffice Router supports both versions 1 and 2 of RIP. RIP Version 2 packets contain information about the complete route to be taken, including the subnet mask.

Triggered RIP and SAP

Triggered RIP and SAP gives you the benefit of dynamically updating routing information without using excessive bandwidth. The HomeOffice Router only sends update messages when it detects a change in its routing or service database. This means that it only sends routing and service data when required, reducing WAN usage and costs, while still being responsive to topology changes.

It is recommended that you use triggered mode on reasonable bandwidth (greater than or equal to 64 Kbps) lines, except where you want to route across more circuits (to more remote sites) than your physical interface can handle. You can only run Triggered RIP and SAP to a certain number of remote sites.

Limitations of Triggered RIP and SAP

Triggered RIP and SAP operation is limited by the following factors:

- the 180-second period after which a route or service is deemed unreachable if it is not possible to connect to the next hop router to the destination (value H); this is configured as the route or hold-down timer
- the number of calls that can be processed in that period

The number of calls that can actually be processed depends on a number of factors:

- the time taken to set up and close a call (value C)

  (for example, five seconds, but it could be longer for international calls)
- the time taken to transfer a RIP or SAP update (value R)

  (for example, five seconds maximum)
- the time the link remains open when transferring data (value I)

  (This is the greater of the following two values: the minimum call timer (value M) or the idle timer.)

If there is no user traffic, each B-channel or virtual circuit can theoretically run Triggered RIP and SAP to the following number of sites per B-channel or virtual circuit.

MAX_SITES = 1 + (H/ (C + (maximum of M, R + I)))

In a real-world environment, other traffic can be transmitted at the same time as RIP and SAP information is being exchanged, so you must take the following factors into account:

- duration of user data
- the preemption timer to each destination (and differing circuit priority)
- the triggered update management timer

  This timer executes every 30 seconds and preempts a circuit whose preemption timer has expired, if preemption is required.

This has an arbitrary reduction factor on the number of remote routers that RIP or SAP can contact within the 180-second period. For this reason, it is recommended that you run Triggered RIP or SAP on no more than the total number of sites that you arrive at using the following equation:

TOTAL_SITES = 1 + 2/3 * (H/ (C + (maximum of M, R + I)))

With ISDN, if you increase the number of B-channels or virtual circuits in use, then you can increase the number of sites to which you can run Triggered RIP and SAP. This means that if you double the number of B-channels, then you can double the number of remote sites. This also applies if you increase the number of virtual circuits on other media types.

Triggered RIP and SAP does not work if you try to run them to more sites than is recommended in this section. You get routes being timed out, many continual retransmissions, and increased WAN costs.

One-way RIP over IPX

The HomeOffice Router includes the ability to ignore incoming IPX RIP updates that are received from the network. Specifically, the HomeOffice Router ignores any RIP updates, either broadcast or triggered, that are received on its ISDN interface.

This feature allows the HomeOffice Router to free up memory that was previously allocated to the IPX RIP table. The HomeOffice Router still responds to RIP requests for broadcast or triggered updates both on the LAN and WAN interfaces.

This feature is applicable in a single-circuit environment (for example, with a HomeOffice Router connected to a remote access switch). In an environment where multiple circuits are involved, it is advisable to allow incoming RIP updates.

Multiple static routes

Introduction

Multiple Static Routes is a cost-saving feature that avoids running RIP over WAN links.The Multiple Static Routes feature applies only to IP and IPX traffic.

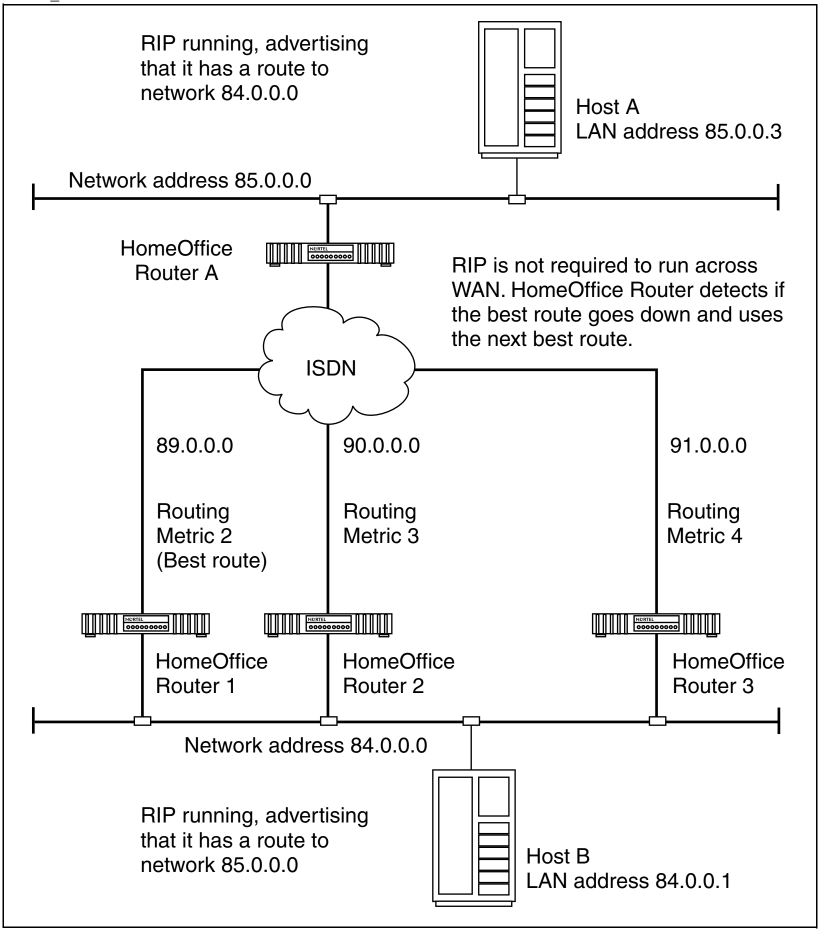
Static routes configuration

You can configure a maximum of three static routes to the same network from a HomeOffice Router. The HomeOffice Router detects if the best route (as defined by the metric value) becomes unavailable, and uses the next best route. If the original best route returns to service, the HomeOffice Router replaces the alternative route. Since the HomeOffice Router determines which route to use, you do not need to run RIP over the WAN links. The HomeOffice Router advertises the active route through RIP (if enabled) on its LAN interface.

Configuration example

The following illustration shows an IP configuration. You can set up multiple static routes in an identical way for IPX.

ISG609_I



When a static route is detected as being down (that is, when the physical link breaks) it can take up to three minutes for an alternative route to be used. This is the length of time that it takes for RIP running on either side of the WAN to broadcast the routing topology change throughout the network. RIP normally works in this way. The three minutes brings some stability to a network based on demand circuits (such as ISDN) since it allows for short periods of time where two routers cannot connect across the demand circuit due to lack of resources.

A note about Automatic Circuit Backup

Do not confuse multiple static routes with Automatic Circuit Backup. Automatic Circuit Backup provides two alternate circuits to the same remote router. In this case, only one route is ever advertised through the routing protocols, regardless of which circuit is in use. It is transparent to all devices (except the two communicating routers), whether the primary or backup circuit provides the connectivity.

Automatic Circuit Backup is

- protocol-independent, so that all of the traffic meant for the primary link is sent over the backup link when it is in operation
- a proprietary feature and is not currently interoperable with any other vendor’s equipment

Choosing between RIP/SAP and multiple static routes

You may decide that static routes can provide the network resilience you require, while avoiding the possible expense of standard RIP and SAP, or the limitations of triggered RIP and SAP.

Multiple static routes are interoperable as they do not rely on any proprietary modifications to existing routing protocols. You can connect a HomeOffice Router set up in this way to any other vendor’s routing equipment.

Multiple static routes apply only to IP and IPX traffic. You can set up both IP and IPX in an identical manner.

You must enable support for Triggered RIP and SAP on a circuit to run Triggered RIP or Triggered SAP over that circuit.

You must enable triggered update circuit management on all circuits set up as static routes if you want the route to disappear from the Forwarding Table while the link is broken.

Multihoming

Introduction

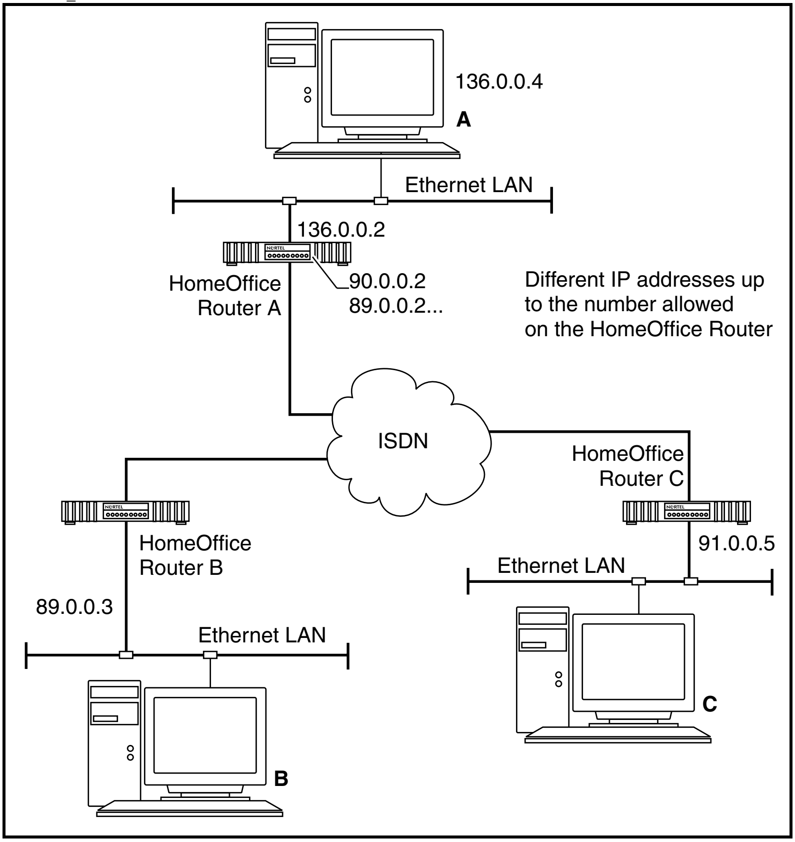
Multihoming means that any LAN or WAN interface can have more than one logical IP network assigned to it. Multihoming allows the HomeOffice Router to run more than one logical network out of a single physical network.

This feature is available on both the Ethernet and ISDN interfaces. The total number of IP addresses on the HomeOffice Router unit must not exceed 10 (shared between the Ethernet and ISDN interfaces).

Example

You can connect two remote ISDN networks using different IP network addresses to a central site via a single ISDN interface at the central site. This is particularly useful when you use a primary rate ISDN interface at the central site. See the following illustration.

ISG604_I


136.0.0.4
A
Ethernet LAN
136.0.0.2
HomeOffice Router A
90.0.0.2
89.0.0.2...
Different IP addresses up to the number allowed on the HomeOffice Router
ISDN
HomeOffice Router C
HomeOffice Router B
91.0.0.5
Ethernet LAN
89.0.0.3
Ethernet LAN
C
B

Filtering

Introduction

Filtering is the process of testing whether a packet needs to be passed onto another network segment. It decreases the level of traffic on your network and is cost-effective because it eliminates most unnecessary traffic between networks.

Bridging filters

You can set up filters based on the destination and source addresses of packets, access groups, packet type, and data content of packets. This helps to reduce the level of traffic passing over the ISDN link or prevents certain users from accessing the ISDN link.

IP filtering

The HomeOffice Router allows IP traffic to be restricted and controlled by using protocol filtering. You can attach filters to any interface or circuit, and they can act on incoming or outgoing traffic.

Each filter holds an access list containing permit and deny conditions called filter elements. Each filter element is a statement defining a set of source and destination addresses, source and destination ports, and protocol information. Packets received or sent by the interface are checked against each filter element until a match is found. The packet is then rejected or accepted for transmission.

SAP filtering

SAP filtering allows you to specify the IPX services that are not broadcasted to other network devices. You can apply filtering on either incoming or outgoing services on the Ethernet or ISDN interface.

Spoofing

Introduction

Spoofing is the process by which the HomeOffice Router prevents meaningless traffic from keeping the network connection open. The settings in the HomeOffice Router's Ethernet interface control some kinds of spoofing that the HomeOffice Router performs. This lets you determine, for some kinds of network traffic, whether the packets are meaningful.

How it works

When you open a connection to a remote network, your computer and other devices on the local and remote networks send a constant stream of network traffic that can keep the network connection open, even when you are not using it for a specific purpose.

It is expensive to keep the network connection open, so the HomeOffice Router closes the connection during idle periods, which are defined as times when no meaningful network traffic is flowing between the local and remote network.

IP spoofing

You can specify whether to spoof the following kinds of network packets:

- TCP KeepAlive packets

  These packets are sent by some older software to keep the TCP connection active during idle periods. Since the HomeOffice Router can open and close the connection as needed, these packets are unnecessary and can be spoofed.

- NetBIOS KeepAlive packets

  These packets are sent by some software to keep the NetBIOS networking active during idle periods. These packets are unnecessary and can be spoofed.

IPX spoofing

The following types of spoofing are available for IPX:

- watchdog spoofing
- SPX spoofing
- NetBIOS probe packet spoofing

Watchdog spoofing

This is a method of keeping costs down, by sending spoof packets from a router on a LAN to another router on the same network. These packets simulate the keep-alive packets normally sent across a WAN from a workstation to the router to maintain the connection. Since spoof packets are sent locally, the transmission costs are lower.

SPX spoofing

SPX spoofing is based on a similar principle to IPX watchdog spoofing, but it is done on a different type of frame, and in both directions.

SPX spoofing significantly reduces network costs because the HomeOffice Router responds locally to probe packets and does not send them across the WAN link. When an SPX connection between a server and client is idle, packets are sent from the server to the client, and vice versa, to ensure that it is still there.

There are three versions of SPX spoofing: V1, V2, or Piggyback. It is recommended that you use Piggyback as a default so that the packets are

- spoofed only when a call is not open
- passed as normal when a call is open

You must use the same version of spoofing at both ends of the link.

NetBIOS probe spoofing

Some software sends these packets to keep the NetBIOS networking active during idle periods. These packets are unnecessary and can be spoofed.

Aggregation

Introduction

The HomeOffice Router allows the ISDN interface to temporarily provide additional bandwidth by using more virtual circuits when available. It allows you to do the following:

- Set up two or more ISDN B-channels to provide more bandwidth.

  This is known as aggregation and is done using PPP Multilink.
- Set thresholds for increasing bandwidth.

  These thresholds determine when additional virtual circuits are opened.

Benefits of bandwidth aggregation

Bandwidth aggregation occurs dynamically on an as-needed basis. Before you begin to set up aggregation, you need to decide at what point you want the second B-channel to open. For example, you may want to open the second channel when the first is at 80% of its maximum throughput. You also need to work out how long you want traffic on the first B-channel to remain at this percentage level before the second channel opens up.

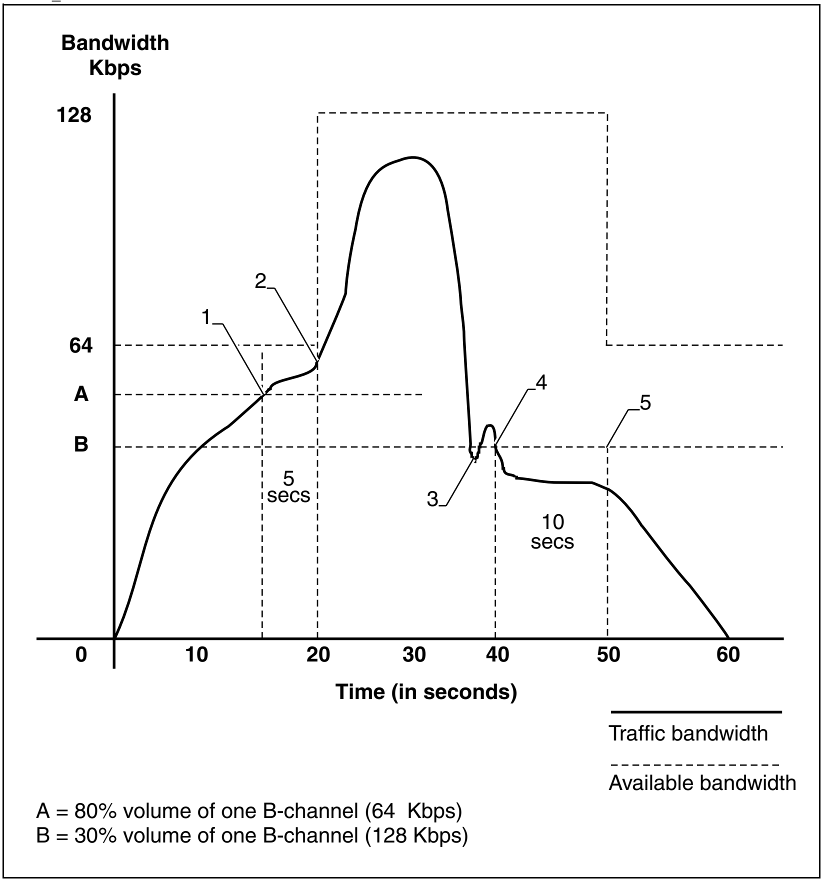
How aggregation works

The following description and illustration explain how aggregation works:

1. When an ISDN call is made, one B-channel opens.
2. In the illustration that follows, Point 1 shows when data reaches the traffic load percentage value. This means that the volume of data has reached the configured percentage value. You can configure the HomeOffice Router to wait for a set length of time before bringing the second B-channel into operation, or you can configure it to open when a sudden burst causes this value to be exceeded. In this case, data volume must exceed 80% volume for a certain length of time (five seconds) before the second B-channel is opened.

3. Point 2 marks the point at which data volume has exceeded the traffic load percentage value for five seconds. The second ISDN B-channel now opens automatically, and remains open until data volume drops below a configurable level. Data is shared equally between the two B-channels.
4. At point 3 in the illustration, traffic decreases temporarily before increasing again. Because bandwidth requirements can change suddenly like this, the second B-channel waits for a period of time before closing down. In the following illustration, this value has been set to 10 seconds. You can set this time to suit your own requirements.
5. At point 4, data drops below the lower traffic load percentage value. Because traffic volume must remain below this threshold for a certain length of time, the second B-channel does not close until point 5 has been reached (10 seconds later).
6. The ISDN link closes when traffic stops.

ISG102_D



Bandwidth Allocation Control Protocol

The Bandwidth Allocation Control Protocol (BACP) allows you to coordinate the addition and removal of B-channels from a bundle interface. This prevents one end from opening another B-channel to accommodate extra data, and the other end from closing it down immediately. When one device wants to increase bandwidth, it contacts the other device and requests that a new B-channel be opened. Both ends must agree to open or close a B-channel before any action is taken.

PPP Multilink Protocol

Introduction

The PPP Multilink Protocol (RFC 1717) is a standardized extension of the Point-to-Point Protocol (PPP) standard. It allows you to

- combine channels into a multilink bundle so that data can be sent at higher rates
- use packet sequencing to order packets
- ensure compatibility between manufacturers of internetworking equipment

PPP Multilink functions

PPP Multilink has the following functions:

- combining links into a multilink bundle
- packet sequencing and ordering
- packet fragmentation over a number of B-channels to reduce latency (this speeds up transmission)
- Address and Control Field Compression
- Protocol Field Compression

PPP Multilink is advantageous because it ensures packet ordering. It also guarantees compatibility with other vendors' equipment because it is an open standard.

Packet fragmentation

You can also enable a feature known as packet fragmentation where larger individual packets are chopped into smaller fragments. This occurs during bandwidth aggregation. These fragments are then distributed among all the channels in use. The receiver at the other end of the links collects the fragments, then reassembles and delivers them in the original order.

Packet fragmentation over a number of links is beneficial because it reduces latency (the length of time a packet waits to receive an acknowledgment from the other end of the link), which decreases transit times and, therefore, speed up transmission.

Multilink compression

Data compression is available for traffic over the ISDN link. By compressing data you can

- reduce transmission costs

  As you can transfer more data down an existing link, you do not need to pay for faster links.
- speed up communication

  The faster transfer of data helps users, while shorter ISDN calls also mean reduced costs.

Data compression can be performed

- on each link in a multilink bundle
- before packets are split onto different links of a multilink bundle

Security authentication

Introductions

The HomeOffice Router supports three types of password authentication:

- Challenge Handshake Authentication Protocol (CHAP)
- Password Authentication Protocol (PAP)
- Shiva Password Authentication Protocol (SPAP)

Challenge Handshake Authentication Protocol

As a part of the PPP suite, CHAP is an authentication protocol that provides additional network security so that a remote access device can authenticate users.

CHAP is secure because it uses a cryptographic handshake to transmit and receive password information.

Password Authentication Protocol

Also a part of the PPP suite, PAP is a protocol that provides additional network security on PPP links. It enables login IDs and passwords to be transmitted over the link so that a remote device can authenticate users.

PAP is less secure than CHAP because it sends the password in plain text across the link.

Shiva Password Authentication Protocol

SPAP is a proprietary security authentication mechanism for PPP negotiation with Intel Shiva LanRover Access Switches.

SPAP is configurable for all circuits, including the listener and default circuits, on a circuit-by-circuit basis. SPAP (like PAP and CHAP) allows you to interoperate between a HomeOffice Router and an Intel Shiva LanRover Access Switch.

There are two main uses for SPAP:

- authentication
- additional functionality for interoperating with other devices

In addition, SPAP offers the following enhanced functionality:

- dial-on-demand
- third-party security (such as SecurID/AssureNet Pathways support)

SPAP passwords are encrypted, meaning increased security.

Caller ID

Caller ID or Calling Line Identification (CLI) is a mechanism for identifying incoming calls. The Router stores *ISDN Address received* entries in its circuit table and checks incoming calls against these addresses. You can use Caller ID to add an extra level of security.

Security authentication and Caller ID

Some incoming calls may not include the Caller ID. Similarly, the Router's Caller ID may not be passed to a device that it is calling. This can occur when you make international calls or when Caller ID is not available and can result in reduced security.

When these circumstances apply, you can choose PAP, CHAP, or SPAP to add an extra level of security on the ISDN link. CHAP and SPAP are the most secure methods because they use encryption to transfer passwords. However, SPAP is a proprietary feature that can only be used to dial in to an Intel Shiva LanRover Access Switch.

Note: If the end user needs to receive incoming calls but does not have Caller ID, you must enable PAP, CHAP, or SPAP.

Section B: Common connection scenarios

In this section

Overview

Introduction

This section provides an overview of three connection scenarios in which the HomeOffice Router can be used.

Connecting to a remote access switch over IP or IPX

A basic configuration is quickly completed by using the Install Wizard. The following list summarizes the steps if you choose to use Local Manager to perform the configuration:

1. Assign an address to the Ethernet interface.
2. Enter the telecommuter’s ISDN numbers on the ISDN interface.
3. Create a circuit to your data network. Associate the circuit with IP or IPX, and enter the address of the remote access switch to which the Router is connecting.

   Note: If you do not assign an IP address to the ISDN interface, unnumbered links are used instead.
4. Create a route to the network identifying the remote access switch’s address or the name of the circuit used to connect to the remote access switch.

Connecting data networks

Hosts on two different networks communicate by sending data packets through a routing device such as the HomeOffice Router.To establish communications between two networks, you must establish the following:

- a physical connection between the routing devices of the two networks
- routing information in each routing device on how to direct packets to the remote networks

HomeOffice Router to RAS over IP

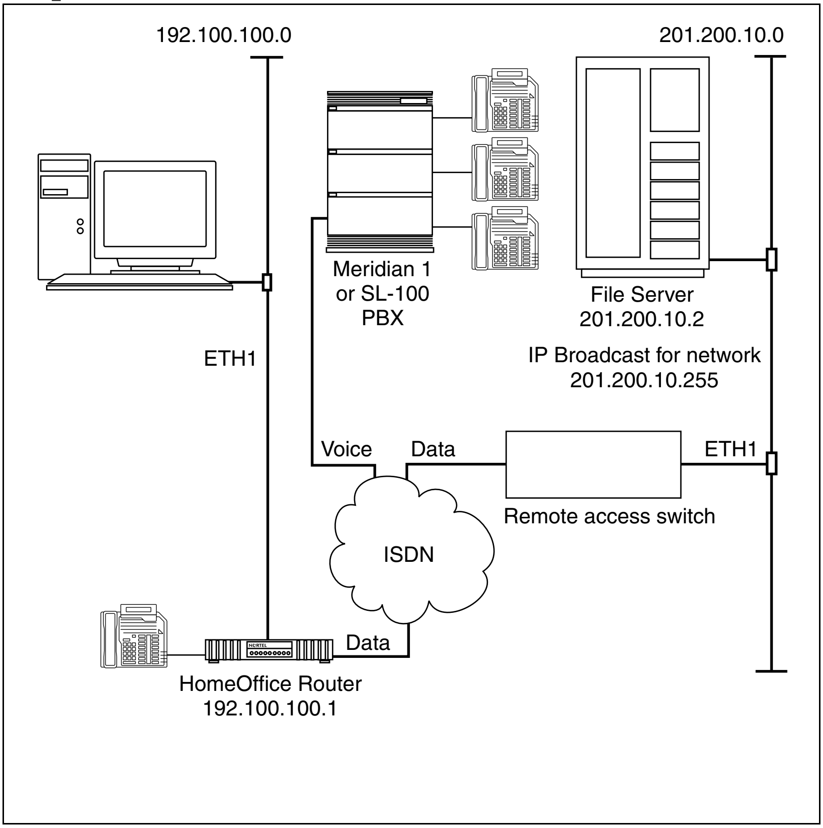
Introduction

This topic describes how to perform a basic configuration for connecting a HomeOffice Router to your remote access switch over IP.

Network diagram

The following illustration shows an example of a HomeOffice Router connected to a remote access switch using IP. A description of the connection configuration follows.

ISG619_I



Configuration at the telecommuter's site

HomeOffice Router configuration

Complete the configuration by using the Install Wizard. For detailed instructions, refer to the *Meridian HomeOffice II User Guide* (NTP 555-8321-205).

In Local Manager, you complete the configuration as follows. (For detailed instructions, see Chapter 3, "Configuring the HomeOffice Router.")

1. On the Ethernet interface

   a Click the Ethernet icon, and then select Properties.

   b Click the IP Properties tab.

   c Enter the IP address. In the previous illustration, it is 192.100.100.1.

   d If you are using Microsoft Networking (but not WINS), click the IP Relay tab.

   e Enter the IP address of the remote file server. In the previous illustration, this is 201.200.10.2.

   Alternatively, enter the broadcast IP address of the remote Microsoft network. In the previous illustration, this is 201.200.10.255.

   f Click OK to reconfigure the Router.

2. On the ISDN interface

   a Click the ISDN icon, and then select Properties.

   b Enter the ISDN telephone numbers assigned to the telecommuter.

   c Click OK to reconfigure the Router.

3. On the ISDN circuit

   a Click the ISDN icon, and then select Circuits.

   b Create a circuit for connecting to the network.

   c On the Numbers tab, enter the ISDN telephone number of the remote access switch. This is the number that the HomeOffice Router needs to connect to the remote access switch.

   d On the security tab, ensure that the appropriate security method is selected (PAP, CHAP, or SPAP). It is recommended that you use SPAP if the HomeOffice Router is connecting to an Intel Shiva LanRover Access Switch.

Ensure that the telecommuter's user name and password are entered in the Local fields. The login ID and password are used for calls initiated by the HomeOffice Router and are authenticated by the remote access switch.

Note: The login ID and password must be the same as the user name and password created in the remote access switch's user list.

e On the Association tab, enable IP and then select Unnumbered links.

f Click OK to reconfigure the Router.

4. In the Routing table

a Click the Admin icon, and then select IP Properties.

b Enter the IP address of the remote network or, in most cases, choose default if only a single connection to a RAS exists.

c Enter the subnet mask of the ISDN network or choose default mask.

d Select the option to enter the IP address of the next hop routing device or enter the name of the circuit used to reach the remote network.

e Change the metric, if necessary. Otherwise, accept the default.

f Click Add to add the route to the table.

g Click OK to reconfigure the Router.

Windows configuration on the PC

Enter the HomeOffice Router's IP address (192.100.100.1) into the gateway field of the TCP/IP Network configuration.

Remote access switch configuration

Configure the remote access switch as follows:

1. Create a user name and password for the telecommuter's HomeOffice Router in the remote access switch's user list.

   The user name and password must be the same as the PAP, CHAP, or SPAP login ID and password in the Local fields on the telecommuter's HomeOffice Router.

   Note: SPAP is recommended if the HomeOffice Router is connecting to an Intel Shiva LanRover Access Switch.

2. Do the following:

IF DIAT for IP on the HomeOffice Router is	THEN
disabled	**1** Configure the telecommuter as a LAN-to-LAN user. **2** Add an IP static route from the remote access switch to the telecommuter's HomeOffice Router.
enabled	**1** Configure the telecommuter as a dial-in user. **2** Assign an IP address to the telecommuter, or configure an IP address pool.

HomeOffice Router to RAS over IPX

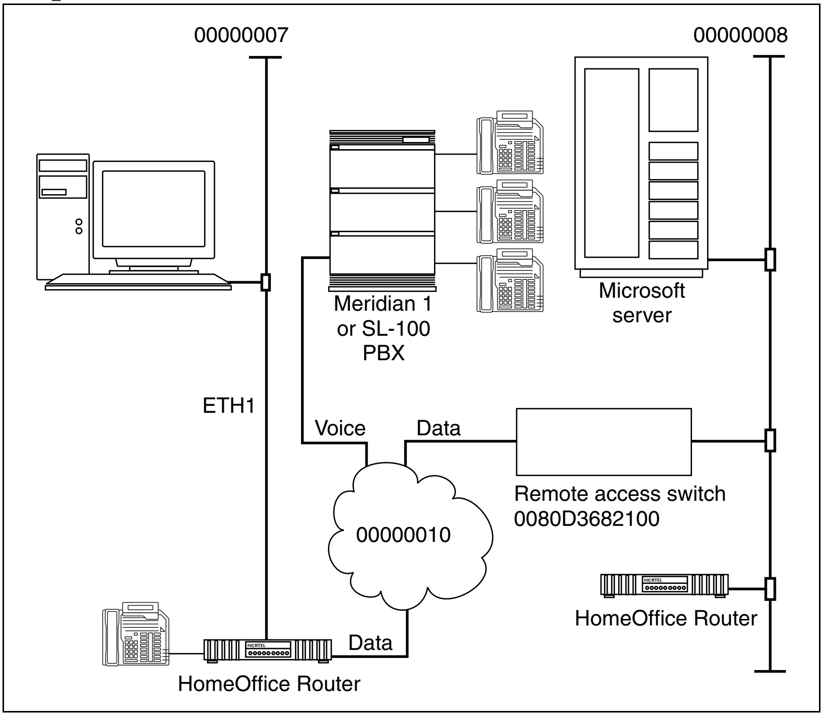
Introduction

This section describes how to perform a basic configuration for connecting a HomeOffice Router to your remote access switch over IPX.

Network diagram

The following illustration shows an example of a HomeOffice Router connected to a remote access switch using IPX. A description of the connection configuration follows.

ISG603_I



Configuration at the telecommuter's site

HomeOffice Router configuration

Complete the configuration by using the Install Wizard. For detailed instructions, refer to the *Meridian HomeOffice II User Guide* (NTP 555-8321-205).

In Local Manager, complete the configuration is completed. (For detailed instructions, see Chapter 3, "Configuring the HomeOffice Router.")

1. On the Ethernet interface

   a Click the Ethernet icon, and then select Properties.

   b Click the IPX Properties tab.

   c Enter the IPX network number. The network number should be the same as the network number of any network servers on the Router's LAN. In the previous illustration, this is 00000007.

2. On the ISDN interface

   a Click the ISDN icon, and then select Properties.

   b Enter the ISDN telephone numbers of the HomeOffice Router.

   c Click the ISDN IPX tab, and then enter the ISDN interface network address. In the previous illustration, this is 00000010.

3. On the ISDN circuit

   a Click the ISDN icon, and then select Circuits.

   b Create a circuit for connecting to the network.

   c On the Numbers tab, enter the ISDN telephone number of the remote access switch. This is the number that the HomeOffice Router needs to connect to the remote access switch.

   d On the security tab, ensure that the appropriate security method is selected (PAP, CHAP, or SPAP). It is recommended that you use SPAP if the HomeOffice Router is connecting to an Intel Shiva LanRover Access Switch.

   Ensure that the telecommuter's user name and password are entered in the Local fields. The login ID and password are used for calls initiated by the HomeOffice Router and are authenticated by the remote access switch.

Note: The login ID and password must be the same as the user name and password created in the remote access switch's user list.

e On the Association tab, enter the node address for the remote access switch. In the previous illustration, this is 0080D3682100.

4. In the Routing table

a Click the Admin icon, and then select IPX Properties.

b Enter the node address of the remote access switch.

c Enter the network address of the ISDN interface.

Windows configuration on the PC

Enter the HomeOffice Router's IPX network address (00000007) into the network address field of the IPX/SPX network configuration.

Remote access switch configuration

On the remote access switch, create a user name and password for the telecommuter's HomeOffice Router in the remote access switch's user list. The user name and password must be the same as the PAP, CHAP, or SPAP login ID and password in the Local fields on the telecommuter's HomeOffice Router.

Note: SPAP is recommended if the HomeOffice Router is connecting to an Intel Shiva LanRover Access Switch.

Limitations and interoperability issues

You should carefully consider IPX usage over an ISDN connection because the IPX protocol is very broadcast-oriented. Service Advertisement Protocol (SAP) broadcasts from the host network cause the ISDN connection to activate on a regular basis. Bandwidth availability across one 56 Kbps channel (assuming a voice channel is configured) and data throughput are affected by the following:

- the number of SAP packets passed
- interval between broadcasts

It is recommended that you implement SAP filtering at the remote access switch to minimize the effects of SAP broadcasts over other IPX data traffic. The filtering of unnecessary print device SAPs, for example, can reduce the number of SAP packets presented to the HomeOffice Router.

Connecting data networks

Introduction

Hosts on two different networks communicate by sending data packets through a routing device such as the HomeOffice Router. To establish communications between two networks, you must establish the following:

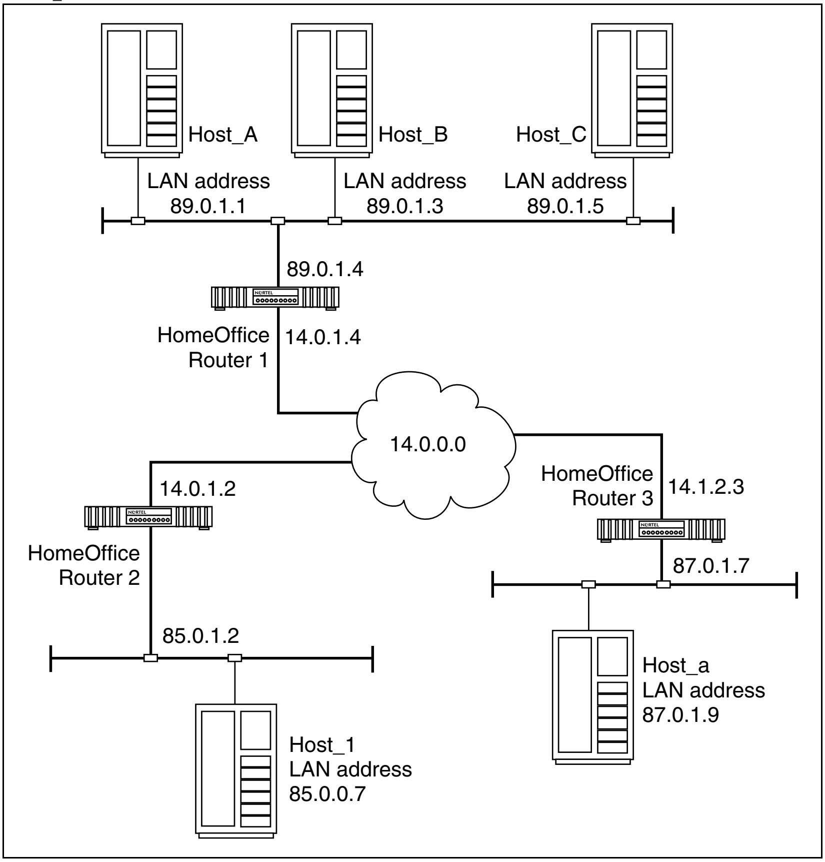
- a physical connection between the routing devices of the two networks
- routing information in each routing device on how to direct packets to the remote networks

Network diagram

In the following illustration, there are two remote data networks that Hosts A, B, and C may want to reach. They are networks 85.0.0.0 and 87.0.0.0. You must tell each of them to send traffic for these destinations through HomeOffice Router 1.

Note: This illustration uses numbered links to connect the networks. You can also use unnumbered links.

ISG608_I



Host routing tables

The routing table that you set up on each host might look like this:

Destination	Router
85.0.0.0	Router_1
87.0.0.0	Router_1

The exact format and contents of your routing table vary from system to system.

Alternatively, if your host computers understand Routing Information Protocol (RIP), you can enable RIP on the Ethernet interfaces of the HomeOffice Router. RIP automatically updates each host's routing table.

For hosts that allow only one router to be specified, the HomeOffice Router tells the host about any other routers, using ICMP redirects.

Using a route utility

In some cases, the system software provides a route utility to allow you to create, edit, and display the routing table. In a UNIX system, you need to set up the destination, the router, and a metric.

For example, you can enter the following command to display the Routing table:

```
netstat -r
```

The display looks similar to the following table:

Destination	Router	Flags	Refcnt	Use	Interface
87	89.0.1.4	UG	0	0	qe0
89	paris	U	57	5431805	qe0
loop	localhost	U	1	447	lo0

Note: You may find that you also need to edit the files in the `/etc/hosts` and `/etc/networks` directories on the host computer. Consult your system's documentation for further information.

Network addresses

LANs connected by routers must have different network addresses. If your networks were previously connected by a bridge, or if your LAN was not previously connected to other LANs (through a WAN), you must ensure that the network address of each LAN is distinct. This may mean that you must change the IP addresses of all of the hosts on one of the LANs to a new network address.

Add an entry for the WAN network to the host's routing table if you want to allow calls from remote HomeOffice Routers to be made into your host. Although calls to a HomeOffice Router can be made into either of its IP addresses, calls from a remote HomeOffice Router use the WAN address. The HomeOffice Router always uses the correct IP address for outgoing calls to the appropriate network.

HomeOffice Router configuration

Using numbered links

To enable the HomeOffice Router to pass traffic to hosts across the WAN using numbered links, configure the following steps in Local Manager (on HomeOffice Router 1):

1. On the ISDN interface
   - a Click the ISDN icon, and then select Properties.
   - b Click the ISDN IP tab, and then enter an IP address. In the previous illustration, this is 14.0.1.4.
2. On the ISDN circuit
   - a Click the ISDN icon, and then select Circuits.
   - b Create a circuit with a meaningful name (such as Router 2 or Router 3 from the previous illustration).
   - c On the Numbers tab, enter the ISDN number used to connect to the remote Router.
   - d On the Association tab, enable IP and select the button below the unnumbered option and enter the IP address of the remote access device.
3. In the Routing table
   - a Click the Admin icon, then select IP Properties.
   - b Enter the IP address for the remote network. In the previous illustration, this is 85.0.0.0 or 87.0.0.0.
   - c Enter the IP address for the next Router in line to that network. In the previous illustration, this is 14.0.1.2 or 14.1.2.3.

Using unnumbered links

To enable the HomeOffice Router to pass traffic to hosts across the WAN using unnumbered links, configure the following steps in Local Manager (on HomeOffice Router 1):

1. On the ISDN interface

   a Click the ISDN icon, and then select Properties.

   b Click the ISDN IP tab, and then ensure that the Unnumbered option is selected.

2. On the ISDN circuit

   a Click the ISDN icon, and then select Circuits.

   b Create a circuit with a meaningful name (such as Router 2 or Router 3 from the previous illustration).

   c On the Numbers tab, enter the ISDN number used to connect to the remote Router.

   d On the Association tab, enable IP and ensure that the Unnumbered option is selected.

3. In the Routing table

   a Click the Admin icon, and then select IP Properties.

   b Enter the IP address for the remote network. In the previous illustration, this is 85.0.0.0 or 87.0.0.0.

   c Enter the name of the circuit that you just created (Router 2 or Router 3).

   d Ensure that the ISDN interface is selected.

Section C: Interoperability issues

In this section

Overview

Introduction

This section describes some interoperability issues that you may need to consider when incorporating HomeOffice Routers into your data network.

Remote access switch

You can use any remote access switch with Meridian HomeOffice II. The remote access switch must have the ability to support the required growth in user connectivity.

You must consider the following issues:

- port availability and contention ratios
- networking features supported by the remote access switch
- protocols that are used
- address allocation

Providing IPX/SPX access when the remote access switch supports only TCP/IP

If you want to use the HomeOffice Router in a network that uses both the TCP/IP and IPX/SPX protocols, your remote access switch must support both those protocols. However, if your remote access switch supports only TCP/IP, this chapter describes how you can install a HomeOffice Router at the network host site and use it to bypass IPX/SPX traffic from a remote HomeOffice Router to the central Local Area Network (LAN).

Note: This configuration is not recommended as a permanent solution because it inhibits the scalability of the telecommuting extension of the Wide Area Network (WAN). You should consider instead using a remote access switch that accommodates various protocols.

ISDN BRI connections at the corporate office

If you want to use a HomeOffice Router and digital telephone while at the corporate office, you need to arrange for ISDN BRI service from your corporate PBX to your desk.

The following examples illustrate why you would need ISDN BRI service to your desk:

- You want to test a HomeOffice Router's configuration before giving it to a telecommuter.
- You want to use the HomeOffice Router to administer or support a Router at a telecommuter's home office.

Remote access switch considerations

Introduction

You can use any remote access switch with Meridian HomeOffice II. However, you need to consider whether the remote access switch has the ability to support the required growth in user connectivity.

You must consider the following issues:

- port availability and contention ratios
- networking features supported by the remote access switch
- protocols that are used
- address allocation

Available ports

You must consider the actual number of remote users who require access and what is expected to be the required number of concurrent users.

The number of concurrent users who must be supported determine

- the number of ports required
- the contention ratio for the access server
- the type and size of remote access switch required

Resources must be available as and when users require. This often means that you require access to central services over varied time zones. You should carefully consider contention ratios with recommendations between 5 and 10:1. A contention ratio of greater than 10:1 is likely to affect users' ability to access resources.

An incorrect contention ratio can result in

- prevention of remote users from gaining access due to the unavailability of ports
- spare ports not being used and therefore not cost-efficient

Analog connections versus ISDN connections

If your current remote access switch supports only analog modem connections, telecommuters may connect the FAX port on their HomeOffice Routers to their computers, and then dial into the network using a dialup adapter (such as Dial Up Networking).

Required features

The following features are recommended to ensure that a remote Meridian HomeOffice II user can gain data access into the main Local Area Network:

- PAP or CHAP security
- an available pool of IP addresses for remote users (required if the corporate site is using DHCP or allocating IP addresses locally from the remote access switch)
- available ISDN PRI or BRI capacity
- redundant power supplies (in chassis switches) (optional)
- Multi-Link PPP support (in standalone switches)
- remote management capability

Note: The availability of a specific feature may depend on whether you use standalone or chassis switches.

Address allocation

In a dialed environment with many remote users, consider using a DHCP server to allocate a pool of IP addresses centrally. The server should be able to act as a proxy agent to direct incoming calls to the server for address allocation. Alternatively, some products have the ability to allocate addresses internally without the need for an additional server, which may provide some cost savings.

Protocols

Wherever possible, IP should be the only protocol to be used across dialed links. Other protocols require some type of spoofing to minimize bandwidth usage. Avoid broadcast bridged protocols or restrict them to particular destinations.

Routing updates can be an issue because they can bring up dialed links. Restrict routing to the LAN with default gateways or use static routes across the WAN.

You can incorporate the HomeOffice Router into your network using either Internet Protocol (IP), Internetwork Packet Exchange (IPX), or both.

It is assumed that your organization already has an Ethernet network in place using either or both of the IP or IPX protocols. If remote sites contain a LAN (more than one workstation), you can implement Dynamic IP or IPX Address Translation (DIAT for IP or IPX) at both the remote and network host sites.

Security

You should carefully consider opening up any data network to remote users, since this provides a potential security threat to customer information. Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) (described below) provide the first level of security and are part of most remote access switches.

In addition to supporting both PAP and CHAP, the HomeOffice Router also supports the Shiva Password Authentication Protocol (SPAP). You can use SPAP if the HomeOffice Router is connecting to an Intel Shiva LanRover Access Switch.

PAP

PAP is a simple password protocol that is part of the IETF suite of protocols. PAP transmits a user’s name and password across a phone line to a central server for authentication. PAP’s password database on the server is encrypted. A user’s password as it travels across the network link is not encrypted.

CHAP

When a remote user calls a server that uses Challenge Handshake Authentication Protocol (CHAP), the server sends back a random challenge (key) to the modem, bridge, or router that initiated the call. The initiating unit uses the key to encrypt the password and returns it to the server. Password snooping is very difficult with CHAP, since the password is encrypted before it is transmitted over the network.

SPAP

The Shiva Password Authentication Protocol (SPAP) is a proprietary security authentication mechanism for PPP negotiation. On the HomeOffice Router, you can configure SPAP for all circuits, including the listener and default circuits, on a circuit-by-circuit basis.

If the remote user's HomeOffice Router connects to a device that is using third-party security authentication (such as a SecurID or Digital Pathways server), you must use SPAP on both the HomeOffice Router and the device to which it is connecting. You must also provide the telecommuter with a security card or other device that provides the passcode needed to access the network.

Note: Outgoing voice calls and incoming data/voice calls are not subject to third-party security authentication.

IPX/SPX access with TCP/IP-only remote access switches

Introduction

If you want to use the HomeOffice Router in a network that uses both the TCP/IP and IPX/SPX protocols, your remote access switch must support both those protocols. This section describes a temporary workaround that you can use if the remote access switch supports only TCP/IP.

Scenario

A telecommuter requires access to both the TCP/IP and IPX/SPX networks. The telecommuter can browse the TCP/IP-based LAN via the existing remote access switch, but cannot access the Novell-based network. The remote access switch at the network host site supports only TCP/IP.

Workaround

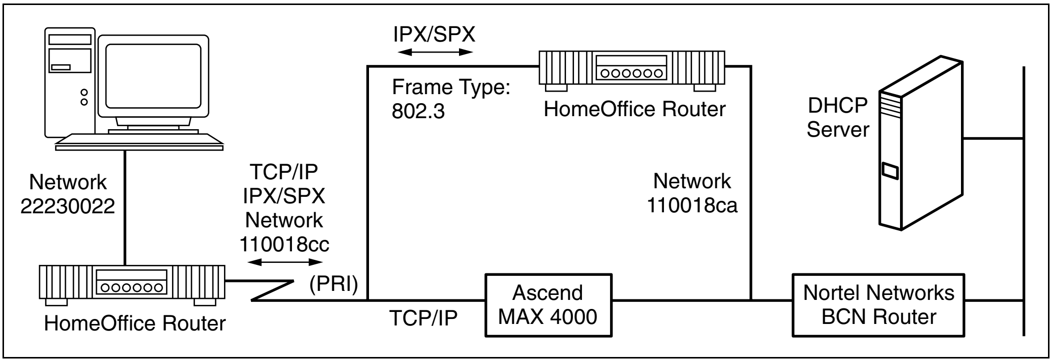
Note: This configuration is not recommended as a permanent solution because it inhibits the scalability of the telecommuting extension of the Wide Area Network (WAN). You should consider instead using a remote access switch that accommodates various protocols.

IPX/SPX traffic bypasses the existing remote access switch and gateway to the central Local Area Network (LAN) through another HomeOffice Router on the central LAN.

Network diagram

The following illustration is an example of an actual network configuration using this workaround.

mhoII01



This configuration accommodates a limited number of users who need to use IPX/SPX. You must provide a separate HomeOffice Router at the network host site for each telecommuter who needs to use IPX/SPX. You must configure each network host HomeOffice Router to interface directly with the central LAN.

To reduce the amount of unnecessary SAP traffic to the network host HomeOffice Router, which could potentially flood its memory, it is recommended that you implement SAP filtering on the remote access switch.

Recommendations

To accommodate potential expansion of IPX/SPX telecommuters, you should use a remote access switch that can pass both TCP/IP and IPX/SPX traffic. Also, consider including configuration of a Microsoft Gateway Services for NetWare (GSNW) server on the network to allow telecommuters to access the Novell file and print servers on the LAN while maximizing the benefits of using TCP/IP across the WAN.

Configuration on the telecommuter’s HomeOffice Router

IP circuit

Configure the TCP/IP circuit on the remote HomeOffice Router using the Install Wizard as described in the *Meridian HomeOffice II User Guide* (NTP 555-8321-205). The DIAT and unnumbered links options are enabled to accommodate the Dynamic Host Configuration Protocol (DHCP) requirements of the WAN network.

With DIAT enabled, the telecommuter's personal LAN can use the DHCP capabilities of the HomeOffice Router to automatically obtain an IP address, subnet mask, and default gateway from the Router.

IPX circuit

Also configure the IPX/SPX circuit on the remote HomeOffice Router using the Install Wizard. Use the same circuit name as configured for TCP/IP.

Choose the DIAT option again, and make the following modifications to the circuit within Local Manager:

1. On the ISDN interface

   a Click the ISDN icon, and then select Properties.

   b Select the IPX Properties tab.

   c Disable RIP by removing the check mark from the associated box.

   d Verify that SAP is enabled.

   e Click OK to reconfigure the Router.

2. On the ISDN circuit

   a Click the ISDN icon, and then select Circuits.

   b Highlight the circuit name and click Change.

   c Click the Security tab, and then verify that the CHAP user name and password are entered in the Local fields.

   d Click the Association tab, and then enable IPX and enter the MAC address of the HomeOffice Router at the network host site.

   e Also on the Association tab, disable RIP for IPX and set SAP for IPX as Triggered.

   f Click OK to reconfigure the Router.

3. On the Admin interface

   a Click the Admin icon, and then select IPX Properties.

   b Click the IPX Routes tab, and then verify that a default route is present.

   The Next Hop node should be the MAC address of the HomeOffice Router at the network host site. The Next Hop network should reference the network address of the WAN/ISDN link (in this example, 110018cc).

   c Click OK to reconfigure the Router.

Configuration on the telecommuter’s Windows PC

Verify that the telecommuter’s PC is configured to obtain an IP address automatically from the network. This is checked within the TCP/IP properties of Network Neighborhood.

To configure the telecommuter’s Novell client on the PC, follow the instructions in the *Meridian HomeOffice II User Guide*.

Configuration on the network host HomeOffice Router

Configure the circuit on the network host HomeOffice Router using the Install Wizard. Since the sole purpose of this unit is to provide an IPX/SPX gateway for the central LAN, DIAT is not required. When prompted for the ISDN number to dial to the remote unit, enter any random seven-digit number to allow the installation process to continue.

Note: The number is removed later in the configuration since this Router does not need to dial out on a circuit.

Verify that the CHAP user name and password of the telecommuter is entered in the Remote fields. When finished with the Install Wizard, open Local Manager and make the following modifications:

1. On the ISDN interface

   a Click the ISDN icon, and then select Properties.
   b Select the IPX Properties tab.
   c Disable RIP by removing the check mark from the associated box.
   d Verify that SAP is enabled.
   e Click OK to reconfigure the Router.

2. On the ISDN circuit

   a Click the ISDN icon, and then select Circuits.
   b Highlight the circuit name, and then click Change.
   c Click the Security tab, and then verify that the CHAP user name and password are entered in the Remote fields.
   d Click the Numbers tab, and then remove the previously entered ISDN number to call and replace it with the word DISABLED.

e Click the Association tab, and then enable IPX and enter the MAC address of the telecommuter’s HomeOffice Router.

f Also on the Association tab, disable RIP for IPX and set SAP for IPX as Broadcast.

g Click OK to reconfigure the Router.

3. On the Admin interface

a Click the Admin icon, and then select IPX Properties.

b Click the IPX Routes tab, and then verify that a default route is present.

The Next Hop Node should be the MAC address of the telecommuter’s HomeOffice Router. The Next Hop network should reference the network address of the WAN/ISDN link (in this example, 110018cc).

c Click OK to reconfigure the Router.

ISDN BRI requirements at the corporate office

Introduction

If you want to use a HomeOffice Router and digital telephone while at the corporate office, you need to arrange for ISDN BRI service from your corporate PBX to your desk.

Reasons why you need ISDN BRI service to your desk

The following examples illustrate why you would need ISDN BRI service to your desk:

- You want to test a HomeOffice Router's configuration before giving it to a telecommuter.
- You want to use the HomeOffice Router to administer or support a Router at a telecommuter's home office.

Configuration requirements

Ensure that the ISDN BRI service is configured with the following items:

- two B-channels providing both voice and data capability

  Both B-channels must be Circuit Switched Voice and Data.
- two directory numbers
- Caller Line Identification
- two Service Profile Identifiers (SPIDs)

Note: If SPIDs are not provided, then you need Multiple Subscriber Numbering (MSN).

For more details about ISDN BRI provisioning, refer to the *Meridian HomeOffice II User Guide* (NTP 555-8321-205). For instructions on configuring an ISDN BRI line from your Meridian 1 or SL-100 PBX, refer to your switch documentation.

Chapter 2

Preparing for implementation

In this chapter

Overview

Introduction

This chapter provides an overview of how to incorporate Meridian HomeOffice II into your data network.

Installation checklists

Review the Installation Checklist—Data Network Manager/Administrator on pages 72 and 73 for an overview of what needs to be done.

Create a network drawing

To help you visualize your network, create a network drawing that shows the following items:

- the devices in your data network (such as remote access switches, routers, and bridges)
- connection paths between those devices
- a label for each device and connection path identifying the network address, ISDN number, and protocol information

This visualization will help you plan your addressing scheme and enable you to set up the network more quickly and easily.

Data entry forms

Review the configuration forms shown in Appendix B at the end of this guide for an overview of the information needed by each telecommuter. You can do one of the following with these forms:

- Complete the configuration forms and give them to the telecommuter with instructions to configure his or her own HomeOffice Router.
- Use these forms to gather the information you need to configure each HomeOffice Router. Then configure the HomeOffice Routers before you distribute them.

Meridian HomeOffice II Page 1 of 2
Installation Checklist—Data Network Manager/Administrator

Check	Task
□	Ensure that a sufficient number of remote access switches supporting ISDN connections are already installed, configured, and working.
□	Determine which network routing protocol is used: IP, IPX, or Bridging.
□	Decide on a security authentication method: CHAP or PAP. If using third-party security authentication or an Intel Shiva LanRover Access Switch, use SPAP. Assign passwords.
□	Configure a user ID and password for each telecommuter in the remote access server.
□	Assign an IP or IPX address to each telecommuter's HomeOffice Router. This becomes the telecommuter's gateway address in the Windows configuration on his or her PC. This IP/IPX address can be a dummy address if you are using DHCP with DIAT. Or, if not, it can be an actual IP/IPX address from your corporate IP/IPX address pool.
□	Identify WINS and DNS server addresses.
□	Obtain ISDN directory numbers and SPIDs (if applicable) for each telecommuter from the coordinator.
□	Configure a circuit on each user's HomeOffice Router to allow you to establish a connection for performing upgrades, maintenance, and so on (recommended).

Meridian HomeOffice II Page 2 of 2
Installation Checklist—Data Network Manager/Administrator

Check	Task
□	If desired, perform an advance configuration of each telecommuter's HomeOffice Router. Test the configuration to ensure that you can establish data and PBX connections. or Complete the network routing and security authentication forms for each telecommuter and give them to the coordinator. The telecommuters perform their own configurations. In either case, ensure that each HomeOffice Router is configured to allow remote administration, maintenance, or upgrades before delivering it to the telecommuter.
□	Ensure that at least one HomeOffice Router is installed at the network host site for remote upgrades, administration, or troubleshooting purposes. Ensure that the administration HomeOffice Router is configured with remote administration circuits so that you can connect to each remote unit, when needed.
□	Record each telecommuter's ISDN number that is assigned to "data" somewhere at the network host site so that you can establish a connection with the remote telecommuter's Router for firmware upgrades and technical support. Create outgoing circuits with this information on the remote access switch.

Creating a network drawing

Introduction

To help you visualize your network, create a network drawing.

What the drawing should contain

The network drawing should show the following items:

- local and wide area networks
- the devices used in each network (such as remote access switches, routers, and bridges)
- connection paths between those devices
- a label for each device and connection path identifying the network address, ISDN number, and protocol information

This visualization will help you plan your addressing scheme and enable you to set up the network more quickly and easily.

Examples

The diagrams shown in the section “Common connection scenarios” on page 39 are abbreviated examples of network drawings.

Planning the HomeOffice Router configuration

Introduction

As network administrator, you are responsible for ensuring that HomeOffice Router configuration is correctly performed. If the configuration is incorrect, the telecommuter cannot access network devices and services.

Configuration methods

You can do one of the following before giving HomeOffice Routers to corporate telecommuters:

- Complete the data entry forms shown in Appendix B at the back of this guide with the information the telecommuters need to connect and work with your network. Include the completed forms in each telecommuter’s HomeOffice Router package. Instruct telecommuters to use these forms to configure their Routers.
- Configure HomeOffice Routers before you give them to the telecommuters. Use the data entry forms to identify the information you need.

Remote access circuit configuration

Regardless of the method you choose for configuring Routers before deploying them, you must ensure that the Router is configured to allow you to establish a remote connection. If you do not do this, and the telecommuter calls you for assistance, you will not be able to connect to his or her Router.

For more details, see “Configuring the HomeOffice Router for remote administration” on page 124.

Configuring the HomeOffice Router in advance

If the configuration is basically the same for all Routers, you can do the following:

1. Create a basic configuration file.
2. Run the Install Wizard for each HomeOffice Router and make the necessary configuration changes.

For instructions on using this method, see “Configuring multiple Routers quickly” on page 90.

Using the data entry forms

The following information describes the data entry forms shown in Appendix B at the back of this guide. Use this guide and the *Meridian HomeOffice II User Guide* (NTP 555-8321-205) to obtain the information you need for completing the forms.

ISDN provisioning information

Telecommuters probably do not know anything about ISDN. If they are required to arrange for ISDN installation in their homes, they must be told

- what information the ISDN service provider needs
- what information the ISDN service provider must give

Before you give the HomeOffice Router—ISDN Provisioning Information forms (see pages 425 and 426) to the telecommuter, *you* must complete Part A. The telecommuter completes Part B.

The ISDN service provider must provide the following items:

- two B-channels providing both voice and data capability
  Both B-channels must be Circuit Switched Voice and Data.
- Caller Line Identification (in the United Kingdom, this is known as Calling Line Identity Presentation [CLIP])
- two directory numbers
- two Service Profile Identifiers (SPIDs)

You need Multiple Subscriber Numbering (MSN) in situations where no SPIDs are provided.

Meridian interface information

You must configure the HomeOffice Router with information about the digital telephone to which the Router will be connected.

You must complete the HomeOffice Router—Meridian Interface Information form (see page 427) and include it with the installation package. Ensure that the information matches what has been configured on the PBX. Otherwise, the telecommuter may not be able to use the telephone.

IP routing, IPX routing, or bridging information

Telecommuters probably do not know anything about networking protocols. *You* must complete one of the following forms before you give it to the telecommuter:

- HomeOffice Router—IP Routing Information (see pages 428 and 429)
- HomeOffice Router—IPX Routing Information (see page 430)
- HomeOffice Router—Bridging Information (see page 431)

These forms contain the questions that you must answer when configuring the HomeOffice Router with the Install Wizard.

To get the information you need to complete these forms, do one or more of the following:

- Read this manual.
- Refer to the *Meridian HomeOffice II User Guide* (NTP 555-8321-205) that is provided with the HomeOffice Router, and run the Install Wizard (to get an idea of what the telecommuter must do).
- Refer to the Install Wizard Online Help topics.

Security authentication information

If your network is using PAP, CHAP, or SPAP security authentication, *you* must complete the HomeOffice Router—Security Authentication Information form (see page 432) before you give it to the telecommuter.

The login ID and password that you provide must be the same as the login ID and password defined for the telecommuter on the remote access switch to which he or she is connecting.

If the remote access switch is to call the telecommuter’s HomeOffice Router, the login ID and password used by that device must be the same as the login ID and password defined on that device.

If additional security authentication (such as SecurID) is being used, ensure that

- you instruct the telecommuter to configure the HomeOffice Router with SPAP
- you provide the telecommuter with a security card (or appropriate device) that contains the passcode needed to access the network
- the user name and passcode are the same as what is defined for the telecommuter on the security server

Planning the configuration of host site remote access switches

Introduction

You must configure the remote access switches at your host site to allow telecommuters to connect to and work with your network.

User lists

Ensure that user lists, if used, contain an entry for each telecommuter. User lists permit login attempts from remote users.

User IDs and passwords

If security authentication will be used, you must ensure that the remote access switch is configured with a user ID and password for each telecommuter.

Ensure that the user ID and password configured on the remote access switch for each telecommuter are identical to the user ID and password configured on the telecommuter’s HomeOffice Router. If they do not match, the telecommuter cannot connect.

Circuits

You must appropriately configure the remote access switch to accept incoming calls from telecommuters.

In addition, you may want to consider configuring outgoing data circuits that will be used for technical support and remote administration purposes.

Deploying the remote units

Introduction

This section identifies what should be provided in each telecommuter's HomeOffice Router package.

ATTENTION

Ensure that the HomeOffice Router is configured to allow you to establish a remote connection. If you do not do this, and the telecommuter calls you for assistance, you cannot connect to his or her Router.

For more details, see "Configuring the HomeOffice Router for remote administration" on page 124.

Package contents checklist

The Package Contents Checklist (see page 422) assures the telecommuter that he or she has received all of the items and information needed to complete the installation and configuration of the telephone, HomeOffice Router, and Windows PC.

If you have opened the HomeOffice Router package to perform advance configuration (or for any other reason), use this checklist to ensure that *you* provide the telecommuter with everything that he or she needs.

Configuration instructions

If you choose to have telecommuters configure their own Routers, ensure that they complete all of the tasks necessary for getting the HomeOffice II product operational. Ensure that the data entry forms shown in Appendix B at the back of this guide are included in the HomeOffice Router package.

Note: If telecommuters need to perform any Local Manager configuration, ensure that you refer them to the appropriate procedures in this guide. You may want to review the procedures to ensure that they provide sufficient information. Provide additional details if required.

Windows PC

To enable a telecommuter's PC to connect through the HomeOffice Router to your corporate data network, you must configure either one or both of the TCP/IP and IPX/SPX network protocols on the PC.

To configure TCP/IP on the PC, you must configure the following:

- the PC's IP address
- the gateway address
- Windows Internet Naming Services (WINS)
- Domain Name Server (DNS)

To configure IPX on the PC, you must enter the IPX address. For Windows NT only, you must provide the preferred server (for NetWare 3.x) or preferred context and tree (for NetWare 4.x). The telecommuter needs this information to log in to the network.

Record the information on the following forms, and then provide it to the telecommuter:

- Windows PC—TCP/IP Network Configuration Information
- Windows PC—IPX/SPX Network Configuration Information

For further details, refer to the "Setting up your PC" chapter in the *Meridian HomeOffice II User Guide* (NTP 555-8321-205).

Chapter 3

Configuring the HomeOffice Router

In this chapter

Overview

Introduction

This chapter explains how to configure the following items:

- ISDN circuits
- Meridian circuit
- TCP/IP networking features, IPX networking features, or both, on the ISDN and Ethernet interfaces

Local Manager

Local Manager is a configuration utility installed on your PC that allows you to install, configure, and monitor your HomeOffice Router. You can use Local Manager to do the following:

- configure the Router to

  — connect to the corporate PBX (Meridian interface)

  — connect to your corporate data network (ISDN and Ethernet interfaces)
- monitor the status of your Router (call statistics and logs)
- perform firmware upgrades (both motherboard firmware and daughterboard firmware, which provide the ability to connect to the corporate PBX)
- perform diagnostics (using ISDN tests, Meridian phone and call tests, and the diagnostics utility)
- perform security authentication when logging into the corporate network, or when accepting calls from a network host
- enable password security for Local Manager access (if desired)

Levels of configuration

You must ensure that the ISDN port is appropriately configured so that circuit configurations will work correctly. The configuration at the circuit level depends on the associated configuration at the ISDN port level to work correctly.

Configuring multiple Routers quickly

You can prepare HomeOffice Routers for deployment by creating a basic configuration file with settings that are the same for all telecommuters. Then you create a custom configuration for each telecommuter by modifying only the settings that are unique to each telecommuter. This chapter provides a guideline for doing this.

ISDN interface and circuits

This chapter explains how to configure the following:

- ISDN interface
- Meridian (PBX) circuit providing digital telephone connection to the corporate PBX
- the following types of data circuits, providing connection to the corporate local area network (LAN):
  - — incoming data circuit for each telecommuter
  - — outgoing data circuit for each telecommuter
  - — outgoing data circuit for administrators (for remote administration and support)

TCP/IP and IPX

This chapter describes TCP/IP and IPX/SPX features, when and why they should be used, and how to configure them with Local Manager.

Levels of configuration

Introduction

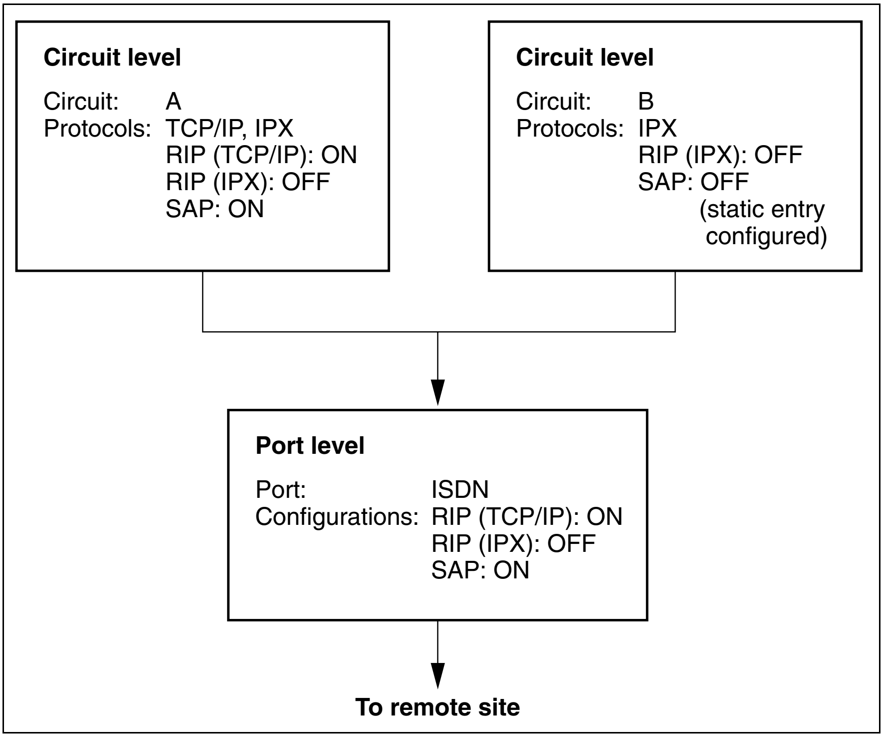
On the HomeOffice Router, specific data configurations are controlled at the ISDN port level and at the circuit level. The configuration at the circuit level depends upon the associated configuration at the ISDN port level.

Ensure that the ISDN port is configured to pass or filter the specific packets so that circuit configurations work correctly.

Example

The following diagram shows the relationship between the ISDN port and circuits.

mhoii05



How it works

The activation of specific settings at the circuit level is only effective if the associated settings at the port level are configured in the same way.

In the previous illustration, Circuit A is configured to send RIP packets for TCP/IP to the remote network. RIP packets are sent only if the ISDN port is also configured to pass RIP packets.

The same principle also applies to SAP packets for the IPX protocol configuration on Circuit A. If SAP is not enabled on the ISDN port, the SAP configuration on the circuit is ignored. As a result, Circuit A does not receive the required SAP information to locate servers on the remote host network.

In Circuit B, although SAP is not enabled to dynamically register service broadcasts to its database table, one or more static entries in the table provide this routing information for the IPX protocol.

About the X.25/D protocol

Introduction

The HomeOffice Router provides three interfaces:

- Ethernet
- ISDN
- X.25

This product release supports only the Ethernet and ISDN interfaces.

What X.25/D is

X.25 over the D-channel (X.25/D) is a communications mechanism that sends packets of data (in a similar fashion to the X.25 protocol) over the signaling or D-channel of the ISDN circuit. This offers a low-cost mechanism to transmit data at relatively low speed, and finds applications in areas such as credit card authorization, alarm monitoring, and so on. This service is being introduced into various countries.

X.25/D and Nortel Networks

The HomeOffice Router contains this feature capability. However, since Nortel Networks has not yet received regulatory approval for this feature in all countries, it has not been enabled.

HomeOffice Router table sizes

Introduction

You should be aware that the HomeOffice Router tables are limited in the number of entries they may contain.

Table sizes

The following table identifies the limits:

Table	Size
circuit table	17 (including the listener circuit)
maximum circuits per interface	17 (including the listener circuit)
number of IP addresses (multi-homed)	10 (shared between Ethernet and ISDN interfaces)
IP routing table: static	32
IP routing table: dynamic	at least 256 (actual limit depends on memory availability)
IP relay forwarding addresses	16
dynamic bridge filter table	2052 entries
packet filter table	100 elements
IPX routing table: static	34
IPX routing table: dynamic	256, with 2 alternatives per route
IPX service table: static	17
IPX service table: dynamic	256

Configuring multiple Routers quickly

Introduction

This section describes how you can prepare HomeOffice Routers for deployment. It is recommended that you do the following using the Install Wizard:

1. Create a basic configuration file.
2. Load the basic configuration file onto each telecommuter’s Router.
3. Modify the basic configuration with settings that are unique to the telecommuter.

Based on whether you configured each telecommuter’s Router or performed an offline configuration, you can do one of the following:

- Distribute the HomeOffice Routers with the configuration files already installed.
- Distribute the HomeOffice Routers and configuration files separately (in which case, the telecommuters must use the Local Manager restore option to load their configuration files to their Routers).

To create a basic configuration

For detailed instructions, refer to Chapter 5, “Configuring the HomeOffice Router,” in the *Meridian HomeOffice II User Guide* (NTP 555-8321-205). The *User Guide* explains how to use the Install Wizard.

1 Decide which aspects of the entire configuration will remain the same for each telecommuter.

See the following table.

Unique for each telecommuter	Identical for all telecommuters
• ISDN switch type (determined by the telecommuter’s ISDN service provider)	• ISDN number of the remote access switch (dependent on the remote access switch’s location)

Unique for each telecommuter	Identical for all telecommuters
• ISDN directory numbers (voice and data) • PBX number (used by the HomeOffice Router to establish connections with the PBX) • PBX security identifier • IP or IPX addresses for the Ethernet and ISDN interfaces • user name and password for security authentication	• number of B-channels used (two) • network protocol used • IP or IPX address of the remote access switch • security authentication method • remote access switch's security authentication user name and password • Meridian password

2 Run the Install Wizard.

Note: You can select a device that is connected to your LAN or PC COM port, or you can perform an offline configuration.

3 Enter the information requested on each screen.

Note: Use generic entries for items that need to be uniquely configured for each telecommuter.

4 Save the configuration under a generic file name in an administration directory on your network.

To create a custom configuration for each telecommuter

1 If you have not already done so, create the basic configuration file (see page 90).

2 Run the Install Wizard again.

3 On the Welcome screen, click Open, and then select the file you saved in step 4 above.

4 Select the device that you want to configure.

5 On each screen, change the settings that are unique to the telecommuter for whom you are configuring the Router.

Note: The basic settings that you entered previously appear as defaults on the screen. Change them as required.

6 On the last Install Wizard screen, click Save.

7 Save the file under a name that is specific to the telecommuter.

8 Using Local Manager, configure the local calling permissions for the telecommuter, if required.

Note: For instructions, see the following:

- "Configuring the PBX (Meridian) circuit" on page 114
- "To enter the security information" on page 118

9 Repeat steps 2 through 8 for each HomeOffice Router that you must configure.

Section A: Using Local Manager

In this section

Overview

Introduction

You can configure the HomeOffice Router by using one of the following:

- Install Wizard to perform the initial configuration
- Local Manager to fine-tune the configuration
- command shell for more advanced configuration

Local Manager

Local Manager is a configuration utility installed on your PC that allows you to install, configure, and monitor your HomeOffice Router. You can use Local Manager to do the following:

- configure the Router to

  — connect to the corporate PBX (Meridian interface)

  — connect to your corporate data network (ISDN and Ethernet interfaces)
- monitor the status of your Router (call statistics and logs)
- perform firmware upgrades (both motherboard firmware and daughterboard firmware, which provide the ability to connect to the corporate PBX)
- perform diagnostics (using ISDN tests, Meridian phone and call tests, and the diagnostics utility)
- perform security authentication when logging in to the corporate network, or when accepting calls from a network host
- enable password security for local manager access (if desired)

Using other configuration tools

In addition to Local Manager, you can also use the following tools to configure the HomeOffice Router:

- Install Wizard
- command shell

Install Wizard

Use the Install Wizard to perform basic configuration for the following:

- ISDN connection
- PBX connection
- IP or IPX routing or bridging
- security authentication using PAP, CHAP, or SPAP

Complete instructions for using the Install Wizard are located in the *Meridian HomeOffice II User Guide* (NTP 555-8321-205), which is located on the HomeOffice II CD-ROM.

Command shell

You can access the command shell by using one of several methods. For instructions on how to use the command shell, see the *Meridian HomeOffice II Command Shell User Guide* (NTP 555-8321-910) on the Meridian HomeOffice II CD-ROM.

Communicating with the HomeOffice Router

With the Install Wizard and Local Manager utilities, you can make changes to the HomeOffice Router's configuration through the Ethernet crossover cable or RS-232 serial cable that is provided with the unit.

You can change the IP address of the HomeOffice Router to the same network as your PC by using one of the following:

- the Install Wizard
- a terminal emulation application (for example, Hyperterminal)

Starting Local Manager

Introduction

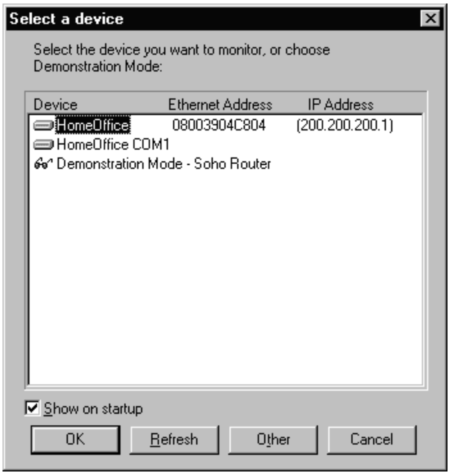
When you start Local Manager, the system prompts you to select the HomeOffice Router to which you want to connect.

To start Local Manager

1 Do the following:

IF you are using	THEN
Windows 3.x	double-click the Local Manager icon in the HomeOffice Program Group.
Windows 95 or Windows NT	click Start > Programs > HomeOffice > Local Manager.

Result: The system prompts you to select a HomeOffice Router from the device selection dialog.



Select a device

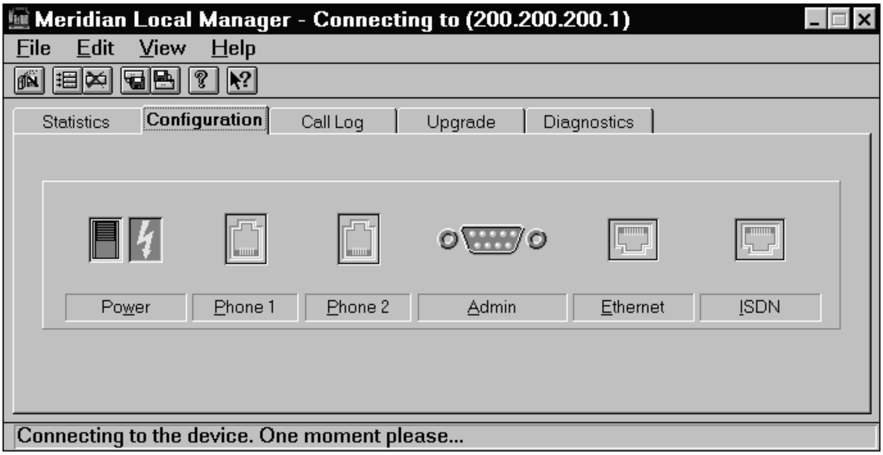
Select the device you want to monitor, or choose Demonstration Mode:

Device	Ethernet Address	IP Address
HomeOffice	08003904C804	(200.200.200.1)
HomeOffice COM1		
Demonstration Mode - Soho Router		

☑ Show on startup

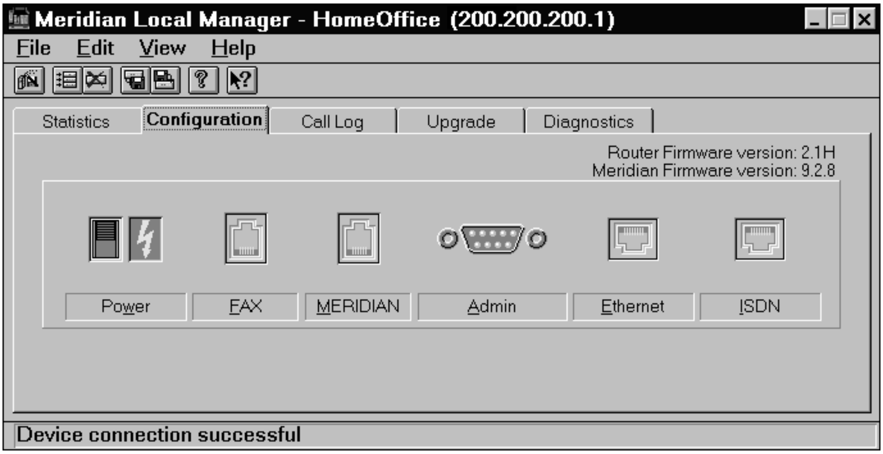
2 Select the device to which you want to connect and click OK.

Result: A screen similar to the following appears, indicating that a connection to the HomeOffice Router is being attempted.



Connecting to the device. One moment please...

Once the connection is successfully established, the screen similar to the following appears.



Router Firmware version: 2.1H
Meridian Firmware version: 9.2.8

Device connection successful

Note: If you are not able to successfully establish a connection with the HomeOffice Router, contact your technical support representative.

Accessing online Help

Introduction

Help is always available while running Local Manager. To obtain a detailed description of what to type or select in each field, see the Local Manager Help topics and the associated glossary.

There are two ways to access the online Help.

Method 1

Do one of the following:

- Click Help (if available) on any Local Manager screen.

  This is the fastest way to get the information you need.
- Click and then drag the ? icon to the area of the screen where you need help.

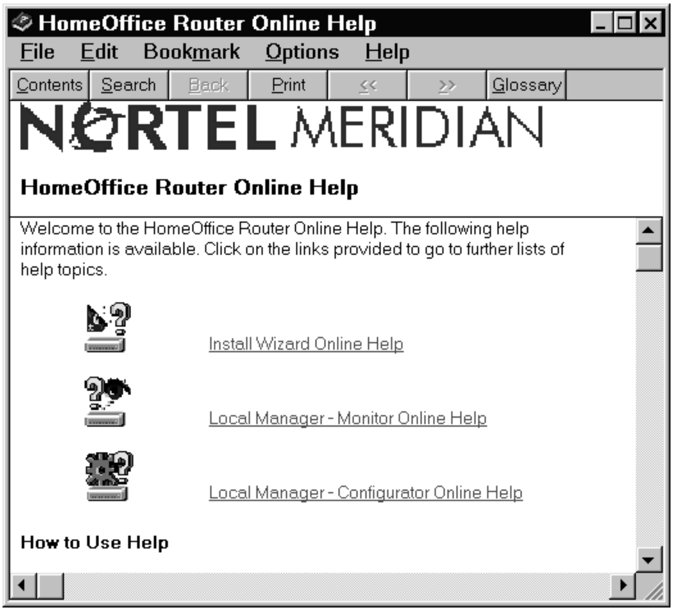
  Context-sensitive help for that particular item appears.

Method 2

Open the suite of Help files.

1 Within Local Manager, select Index from the Help menu.

Result: The HomeOffice Router Online Help window appears.



HomeOffice Router Online Help
File Edit Bookmark Options Help
Contents Search Back Print << >> Glossary
NORTEL MERIDIAN

HomeOffice Router Online Help

Welcome to the HomeOffice Router Online Help. The following help information is available. Click on the links provided to go to further lists of help topics.

Install Wizard Online Help

Local Manager - Monitor Online Help

Local Manager - Configurator Online Help

How to Use Help

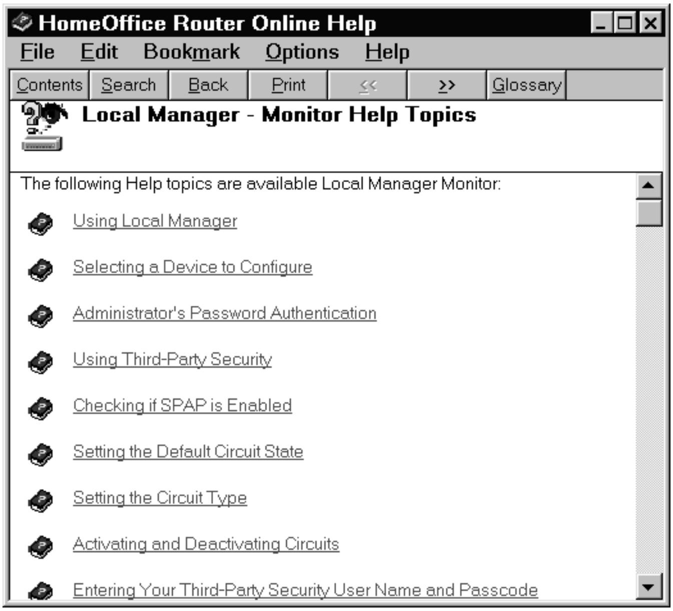
Note: This window provides you with access to Install Wizard Help topics as well.

2 Click one of the following Help topics:

- Local Manager - Monitor Online Help to see topics related to monitoring the status of the HomeOffice Router
- Local Manager - Configurator Online Help to see topics related to configuring the HomeOffice Router

Result: The list of Help topics appears.

Note: The following example is the list of topics for Monitor Online Help.


HomeOffice Router Online Help
File Edit Bookmark Options Help
Contents Search Back Print << >> Glossary

Local Manager - Monitor Help Topics

The following Help topics are available Local Manager Monitor:

- Using Local Manager
- Selecting a Device to Configure
- Administrator's Password Authentication
- Using Third-Party Security
- Checking if SPAP is Enabled
- Setting the Default Circuit State
- Setting the Circuit Type
- Activating and Deactivating Circuits
- Entering Your Third-Party Security User Name and Passcode

3 Click the topic of interest.

Section B: Configuring the ISDN interface and circuits

In this section

Overview

Introduction

This section explains how to configure the following items:

- ISDN interface
- Meridian (PBX) circuit providing digital telephone connection to the corporate PBX
- the following types of data circuits, providing connection to the corporate local area network (LAN):
  - — incoming data circuit for each telecommuter
  - — outgoing data circuit for each telecommuter
  - — outgoing data circuit for administrators (for remote administration and support)

ISDN interface

The ISDN interface consists of the ISDN telephone numbers and SPIDs assigned to each telecommuter, as well as a description of the ISDN service being provided by the ISDN service provider to the telecommuter.

The ISDN Test utility on the ISDN properties ISDN Test tab allows you to check that the Router is correctly configured for the type of switch (exchange) to which it is being connected. To test the ISDN line, you must enter the directory number of the ISDN interface.

Circuits

A circuit is a logical or physical connection between two points on a wide area network (WAN). You can give circuits names for easy reference. The HomeOffice Router stores information about circuits in its circuit table.

On the HomeOffice Router, you can create circuits on the ISDN interface by using the Install Wizard, Local Manager, or the `network isdn2 circuit` command in the command shell.

You must name each ISDN circuit that you set up. You can then use this name to refer to the circuit when you set up protocol-specific information.

Supported circuit types

HomeOffice II supports the following types of circuits:

- data circuit

  The data circuit is used to make data calls to network devices at the corporate site. A data circuit is used by the ISDN interface on the HomeOffice Router.

- fax circuit

  The analog phone (FAX) port on the HomeOffice Router uses the fax circuit to connect voice calls (if a telephone is used), or to send or receive faxes (if a fax machine is used).

- voice circuit

  The digital telephone (connected to the MERIDIAN port on the HomeOffice Router) uses the voice circuit (known as the Meridian circuit in Local Manager, or PBX circuit in the command shell) to connect to the corporate PBX.

Call types and circuit selection

The HomeOffice Router supports the following types of calls (both incoming and outgoing):

- data
- voice

Outgoing calls are routed according to the action taken by the telecommuter. See the following table.

IF the telecommuter	THEN the outgoing call is routed over
picks up the digital telephone handset	the voice (Meridian) circuit.
initiates a LAN connection with the PC	the data circuit.

IF the telecommuter	THEN the outgoing call is routed over
initiates a call on the device associated with the FAX port	the fax circuit.

Incoming data and voice calls are distinguished by the bearer capability, which is identified as either “speech” or “unrestricted digital 56 Kbps or 64 Kbps.” When the HomeOffice Router receives an incoming call, the bearer capability and called directory number are evaluated to determine where it should be routed: to the digital telephone, the analog telephone or fax machine, or the HomeOffice Router itself.

Bearer capability is unrestricted digital 56 Kbps or 64 Kbps

If the bearer capability is unrestricted digital 56 or 64 Kbps, the called number is evaluated and the call is routed as follows:

IF the number	THEN
matches the voice circuit	the call is routed to the digital telephone (HomeOffice Router MERIDIAN port).
does not match the voice circuit	the call is routed to the data circuit (HomeOffice Router ISDN port).

Speech

If the bearer capability is speech, the called number is evaluated and the call is routed as follows:

IF the number	THEN
matches the voice circuit	the call is routed to the digital telephone (HomeOffice Router MERIDIAN port). ***Note:*** The call is considered to be a local call.
matches the fax circuit	the call is routed to the device connected to the HomeOffice Router FAX port.

Configuring data circuits

If you, as network administrator, are configuring HomeOffice Routers for telecommuters, you must configure the following on each Router:

- an outgoing data circuit

  Telecommuters use outgoing circuits to connect to your data network.
- an incoming data circuit

  Incoming circuits accept calls from your network for technical support or remote administration purposes.

In addition, you must configure an outgoing data circuit on your network HomeOffice Router for establishing a connection with a telecommuter's HomeOffice Router.

Limitations

When you configure circuits that will be used for remote administration or technical support, remember the following:

- You can configure a maximum number of 17 circuits on each Router, including the listener circuit.
- You can configure a maximum of 32 static routes.

Alternatives

If you have more sites to administer than is allowed by the circuit and routing tables, you can do one of the following:

- Modify an existing circuit each time you want to connect to a site that is not in your circuit table.
- Use a remote access switch to dial the remote site (establishing a LAN-to-LAN connection).

  For instructions, refer to your remote access switch documentation.
- Use Telnet to connect to the remote site.

Configuring the Meridian circuit

The Install Wizard configures the following items in the Meridian circuit:

- the ISDN voice circuit telephone number
- the Direct Inward Dial (DID) number to call the PBX
- PBX security access codes (if used)

If telecommuters will be allowed to make local calls over their ISDN lines, you must perform the following additional configuration with Local Manager:

- Assign the appropriate local calling permissions.
- Change the Meridian password.

  The password prevents telecommuters from accessing Local Manager and changing local calling permissions. (For instructions, see “Changing the Meridian password” on page 389.)

For instructions on configuring the Meridian circuit, see “Configuring the PBX (Meridian) circuit” on page 114.

Fax circuit

The FAX port is automatically configured when its ISDN number is identified in the Install Wizard. You must inform the telecommuters that this ISDN number is designated as their fax number.

Configuring the ISDN interface

Introduction

The ISDN interface consists of the ISDN telephone numbers and SPIDs assigned to each telecommuter, as well as a description of the ISDN service being provided by the ISDN service provider to the telecommuter.

Directory numbers/ISDN addresses

A directory number is the address or telephone number for the ISDN line assigned by the ISDN service provider or telephone company.

The number of directory numbers allocated depends on which service is being used. If an NI-1 line or a 5ESS Custom Multipoint line is used, one directory number is assigned per B-channel. Otherwise, only one directory number is assigned per device.

Note: To use Meridian HomeOffice II, you need two directory numbers.

Dialing prefixes

Based on the service provider, the telecommuter may be required to include a digit to get an outside line, an area code, and a long distance prefix. For example, the telecommuter may need to dial 916273331234. The parts of this number are as follows:

Digit for an outside line	Long distance prefix	Area code	Telephone number
9	1	627	3331234

Service Profile Identifiers (SPIDs)

When ordering an ISDN service, the service provider needs to know which ISDN features are required (for example, Caller ID). This is known as a service profile. The service provider then allocates a unique Service Profile Identifier (SPID) that allows the telecommuter to use these particular features.

Based on the ISDN variant, either no SPIDs, one SPID, or two SPIDs are assigned to the ISDN line.

Note: Only service providers in North America allocate SPIDs.

Directory number and ISDN tests

The ISDN Test utility within the Local Manager ISDN properties allows you to check that the Router is correctly configured for the type of switch (exchange) to which it is being connected.

If you want to perform a test on the ISDN line, enter a telephone number to use in the call test. Enter the digits as they would be entered on the telephone keypad to make this call. If the local exchange office requires you to dial an access code (for example, dial 9) for your ISDN service, include this number in the dialed digits.

If you are using the ISDN variants 5ESS Custom Multipoint, National ISDN-1, or National ISDN-2, ensure that you enter the SPID (or SPIDs) before you start the ISDN test.

The ISDN Loopback test requires two B-channels on the ISDN line. You cannot use the loopback test if the line is provisioned with only one B-channel.

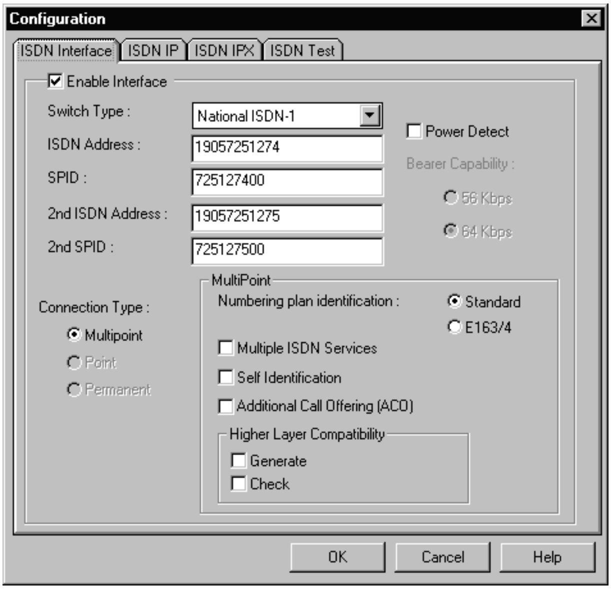
For instructions on how to perform the ISDN tests, refer to the *Meridian HomeOffice II User Guide* (NTP 555-8321-205).

To configure the ISDN interface

1 Click the ISDN icon

2 Select Properties from the pop-up menu that appears.

Result: The Configuration screen appears.



☑ Enable Interface

Switch Type : National ISDN-1

ISDN Address : 19057251274

SPID : 725127400

2nd ISDN Address : 19057251275

2nd SPID : 725127500

□ Power Detect

Bearer Capability : ○ 56 Kbps ● 64 Kbps

Connection Type : ● Multipoint ○ Point ○ Permanent

MultiPoint

Numbering plan identification : ● Standard ○ E163/4

□ Multiple ISDN Services

□ Self Identification

□ Additional Call Offering (ACO)

Higher Layer Compatibility

□ Generate

□ Check

3 Complete the fields as described in “ISDN interface field descriptions” below.

4 Click OK.

Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

ISDN interface field descriptions

Field	Description
Enable Interface	Click the check box to enable the ISDN interface. **Note:** An ISDN address must be assigned for the interface to be enabled.

Field	Description
Switch Type	Select the appropriate ISDN variant from the Switch Type list box. **Note:** You need two directory numbers. The only switch types that support two directory numbers are Euro-ISDN, 5ESS Custom, and National ISDN-1.
Power Detect	When selected, the Router detects whether there is power on the ISDN line. You can use Power Detect to determine if there is a physical connection to the ISDN switch. (The ISDN switch is the switching equipment used by the local telephone exchange for their ISDN service.) If you are connected to an NT-1, ensure that the check box is blank. If you are using a Private Automatic Branch Exchange (PABX), consult your PABX manual to see if power detection is supported. If you are *not* using an NT-1, you must ask your telephone company if the S/T interface that they are providing supports power detection. If you are unsure about what to select, ensure that the check box is blank. This is the most common setting.
ISDN Address	Enter the full directory number provided by the ISDN service provider for the ISDN line. See “Dialing prefixes” on page 107 for more details. When entering an area code, always enter it directly before the main telephone number. Do not use a hyphen (-) as a separator because hyphens are reserved for sub-addressing. If you use sub-addressing, add the sub-address to the end of the number, separated by a hyphen.
SPID	Enter the Service Profile Identifier provided by the ISDN service provider. The SPID can be up to 20 digits in length.

Field	Description
Bearer Capability	The Bearer Capability options for the ISDN interface are dimmed and cannot be selected. You can, however, change the bearer capability on any ISDN circuit. To do this, select the ISDN circuit, then select the required setting in the Outgoing Call Type section on the Circuit tab.
2nd ISDN Address	See ISDN Address.
2nd SPID	See SPID.
Connection Type	Select the connection type required for the ISDN line. Once you have done this, more configuration options appear depending on which connection type you have chosen. If you select Point or Multipoint, you can configure the following: • Numbering Plan Identification • Multiple ISDN Devices • Self Identification • Additional Call Offering • Higher Layer Compatibility If you select Permanent, Local Manager deletes any circuits that are defined.
Numbering plan identification	If using Euro-ISDN and connecting to a PABX, you must adjust the ISDN configuration so that the Siemens Octopus PABX can recognize the numbering plan that the Router is using. • E163/4 PABX: Click this option if you are attaching your Router to a Siemens Octopus. • Standard: Click this option if you are not using this type of PABX.

Field	Description
Multiple ISDN Services	This option allows several devices, such as telephones, faxes, routers and so on, to be attached to one ISDN line but have different numbers. For example: 705 248 2001 = Telephone 705 248 2002 = Telephone answering machine 705 248 2003 = Fax Each device can then listen to all of the incoming calls on the line, but accepts and replies only to calls sent directly to its individual number. If you ordered Multiple Subscriber Numbering from the service provider, it is unnecessary to select the check box here to enable the service. However, you should select the check box if your Router is not the only device on the ISDN bus.
Self Identification	You should normally disable this feature as the network usually provides the calling ISDN number to the remote device. However, in some circumstances (especially when using a PABX), you should enable it. This tells the Router to provide its own ISDN number in outgoing calls. This is useful if the PABX does not provide this service.
Additional Call Offering (ACO)	Select this option if you want to enable Additional Call Offering (ACO). With ACO enabled, if you are using both B-channels for data transmission and the Router detects an incoming voice call, a single data channel is dropped for the voice call to be accepted. Otherwise, the voice call is rejected. **Note:** Enable this option if ACO is provided on the ISDN line and you are experiencing connection problems.

Field	Description
Higher Layer Compatibility	If the network in your country supports Higher Layer Compatibility (HLC), extra information is provided in calls, such as whether a call is from a fax machine, telephone, or Group 4 Fax, is a video conference call and so on. Select Generate when the remote device being connected to is on an ISDN bus with multiple types of devices. All the devices on the ISDN bus must be capable of checking Higher Layer Compatibility or the connection fails. **Note:** HLC is not very common and you may find that you have to use Multiple ISDN Devices service or sub-addressing to achieve the same effect. Select the Check option if the Router that you are configuring is on an ISDN bus with multiple devices that can check for HLC.

Configuring the PBX (Meridian) circuit

Introduction

The Meridian circuit is the connection path between the HomeOffice Router and the HLC port on the corporate PBX. Meridian circuit configuration consists of three screens:

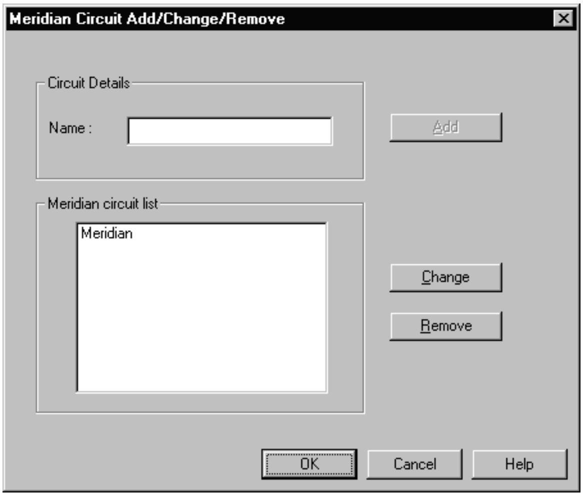
- Connection tab: Used to enter the circuit details, such as the PBX telephone number and minimum call duration and idle timers. See page 114.
- Security tab: Used to set security access levels required by the central PBX and to indicate whether local calls are authorized on the digital telephone. See page 118.
- Meridian tab: Used to define the program function key on the digital telephone that will be used as the Online/LC key. See page 121.

Note: You can only configure one Meridian circuit on the HomeOffice Router. Multiple PBX circuits are not supported.

To enter the connection information

1. Click the MERIDIAN icon.
2. Select Circuits from the pop-up menu that appears.

   Result: The Meridian Circuit Add/Change/Remove screen appears.


Meridian Circuit Add/Change/Remove

Circuit Details

Name :

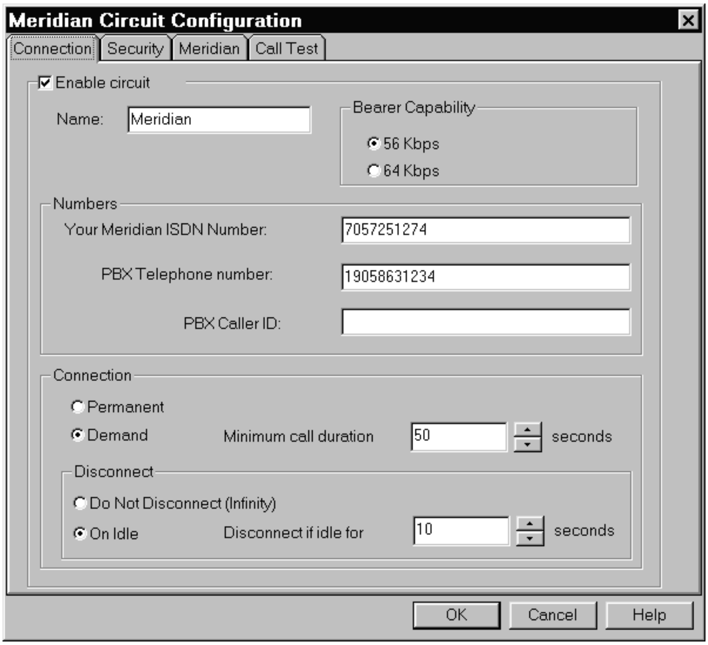
Meridian circuit list

Meridian

3 Select Meridian from the circuit list.

4 Click Change.

Result: The Meridian Circuit Configuration screen appears.


Meridian Circuit Configuration

Connection | Security | Meridian | Call Test

☑ Enable circuit

Name: Meridian

Bearer Capability

● 56 Kbps

○ 64 Kbps

Numbers

Your Meridian ISDN Number: 7057251274

PBX Telephone number: 19058631234

PBX Caller ID:

Connection

○ Permanent

● Demand Minimum call duration 50 seconds

Disconnect

○ Do Not Disconnect (Infinity)

● On Idle Disconnect if idle for 10 seconds

5 On the Connection tab, complete the fields as described in “Connection tab field descriptions” below.

6 Continue with “To enter the security information” on page 118.

Connection tab field descriptions

Field	Description
Enable circuit	Ensure that this box is checked. This indicates that the circuit is online and able to both generate and accept incoming calls.
Name	This is the name assigned to the circuit. Do not change it.
Bearer Capability	Click either 56 Kbps or 64 Kbps to indicate the speed of the ISDN line.
Your Meridian ISDN Number	This is the ISDN telephone number assigned to the digital telephone.
PBX Telephone number	This is the telephone number of the data channel on the central PBX. Ensure that required dialing prefixes are entered (such as 1 for long distance).
PBX Caller ID	This is the caller ID signature required on all incoming calls from the central PBX. It can be left blank to indicate that no caller ID check should be performed. If you want caller ID effective, enter an appropriate number. **Note:** This is usually the phone number of the central PBX.
Connection	Select one of the following connection types: • Permanent: The ISDN connection to the central PBX remains up all the time. If you select Permanent, you cannot configure the minimum call duration and idle timers.

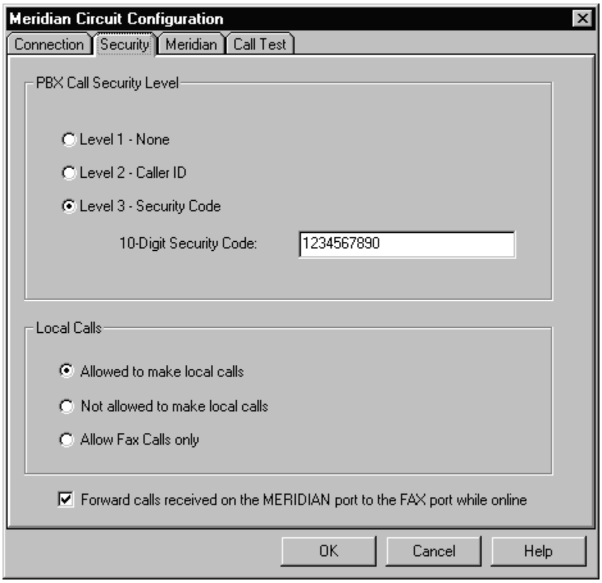
Field	Description
Connection (continued)	• Demand: The ISDN connection to the central PBX is established only when it is required. That is, the connection is activated when an off-hook signal is detected from the digital telephone. Likewise, the connection is removed by the detection of an on-hook signal. Selecting a demand circuit type allows you to configure the minimum call duration and idle timers.
Minimum call duration	This specifies the minimum period of time that a demand circuit should remain active. This feature can be useful in cases where an ISDN service provider charges a minimum fee for a call (say a standard fee for a call of 60 seconds). This means that each time a call is opened, and the call is used for only 20 seconds, your organization is charged for the full 60 seconds. You can, therefore, use this option to set the minimum call duration time to 60 seconds in this example. This allows more calls to be made within the specified time period and, at the same time, only be charged for one ISDN call because the original ISDN call remains active. You can enter a value between 0 and 3600 seconds. The default is 50. **Note:** This option is unavailable for permanent circuit types.
Disconnect	Select the disconnection type. If you select Do Not Disconnect, you cannot enter the idle timer.
Disconnect if idle for	This specifies the period of time that a demand circuit remains active after an on-hook signal is detected from the digital telephone. This option is useful if saving on connection times is a priority.

Field	Description
Disconnect if idle for (continued)	If you set this to 60 seconds, then an ISDN call remains live for 60 seconds after the call is finished. If another number is dialed during this time, the telecommuter does not have to go through the ISDN call setup procedure again. Conversely, it is undesirable to set this value too high if you want to save on tariff costs. That is, presumably it is undesirable to have a connection established if telecommuters leave their workstations for considerable lengths of time. You can enter a value between 0 and 3600 seconds. The default is 10. This option is unavailable to permanent circuit types.

To enter the security information

1 Click the Security tab.

Result: The Security tab appears.



PBX Call Security Level

○ Level 1 - None

○ Level 2 - Caller ID

● Level 3 - Security Code

10-Digit Security Code: 1234567890

Local Calls

● Allowed to make local calls

○ Not allowed to make local calls

○ Allow Fax Calls only

☑ Forward calls received on the MERIDIAN port to the FAX port while online

2 Complete the fields as described in "Security tab field descriptions" below.

Note: Some fields are protected by the Meridian password. For more information about the Meridian password, see "Changing the Meridian password" on page 389.

3 Continue with "To select the Online/LC key" on page 121.

Security tab field descriptions

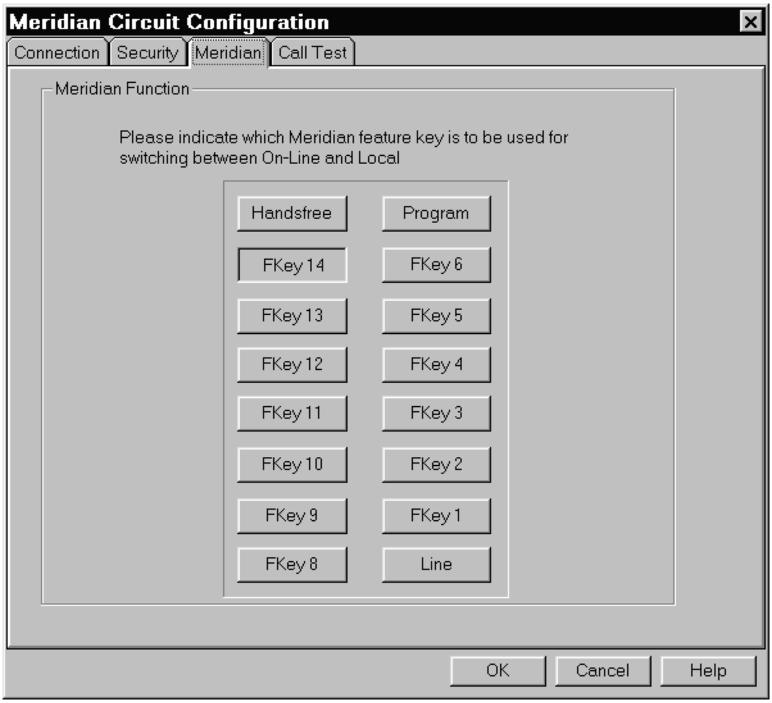
Field	Description
PBX Call Security Level	Use this field to set security access levels required by the central PBX. • Level 1 - None: No restrictions are necessary. • Level 2 - Caller ID: Outgoing calls will are only accepted if a correct caller ID is detected. • Level 3 - Security Code: Outgoing calls are only accepted if a correct security code is detected.

Field	Description
10-Digit Security Code	If you selected Level 3 - Security Code during Install Wizard configuration for the Meridian circuit, then the security code entered displays here. This code is passed to the central PBX when communications are established.
Local Calls	**Note:** The Meridian password protects the following options. For more information about the Meridian password, see “Changing the Meridian password” on page 389. • Allowed/Not allowed to make local calls: Select this option to enable or disable outgoing local calls via an analog phone, fax machine, or Meridian phone. • Allow Fax Calls only: Select this option to enable outgoing calls via a fax machine or analog phone and disable outgoing local calls over the Meridian phone.
Forward calls received on the MERIDIAN port to the FAX port while online	**Note:** The Meridian password protects this option. For more information about the Meridian password, see “Changing the Meridian password” on page 389. When selected, the Router redirects calls received on the ISDN number to the FAX port if the digital telephone is online. This option acts as a courtesy feature, allowing personal calls to be redirected when the digital telephone is online. **Note:** If the FAX port is connected to a fax machine, only incoming fax calls should be redirected.

To select the Online/LC key

1 Click the Meridian tab.

Result: The Meridian tab appears.



Please indicate which Meridian feature key is to be used for switching between On-Line and Local

2 Select the key that is to be configured as the Online/LC key on the digital telephone.

Use the Online/LC key to switch between online and local (offline) modes.

Note: You must select a feature key from one of the numbered feature keys. You cannot select “Handsfree,” “Program” or “Line.”

3 Click OK twice.

Result: You return to the Configuration tab.

Configuring an outgoing data circuit for the telecommuter

Introduction

As network administrator, you should configure a data circuit for the telecommuter before the Router is deployed into the field. The telecommuter uses this outgoing circuit to connect to the corporate data network.

To create the outgoing circuit

The quickest way to configure an outgoing circuit for the telecommuter is to run the Install Wizard and configure a basic configuration file for all telecommuters on your network. Once this is done, you can use the Install Wizard to do the following:

1. Open the basic configuration file.
2. Change settings specific to a telecommuter.
3. Save the configuration under a file name (using the .IWZ file extension) specific to the telecommuter.

You can then load this modified configuration file on the telecommuter’s PC and subsequently restore it to his or her Router.

For instructions, see the following topics in the “Configuring the HomeOffice Router” chapter of the *Meridian HomeOffice II User Guide*
(NTP 555-8321-205):

- “Entering IP information”
- “Entering IPX information”
- “Entering Bridging information”

ATTENTION

If you have already configured the ISDN interface, the Meridian circuit, or any other information for the telecommuter, ensure that you open the telecommuter's configuration file with the Install Wizard. If you run the Install Wizard without opening a configuration file, the settings you have already configured will be overwritten.

You can open an existing configuration file by clicking Open on the Install Wizard Welcome screen.

Where to get more information

For descriptions of fields on the Circuit Configuration screens, see "Data circuit configuration reference" on page 139.

Configuring the HomeOffice Router for remote administration

Introduction

Before a HomeOffice Router is deployed into the field, you (the network administrator) should configure a circuit that would be used to remotely access over ISDN, the telecommuter's Router for firmware upgrades, administration, troubleshooting, technical support, and so on.

Use Local Manager to configure both the telecommuter's Router and the Router at the network host site.

Administration tips

You can configure the administration HomeOffice Router with up to 16 circuits plus the listener circuit. You can potentially have 14 remote access circuits configured on the router in addition to the already configured *admin* and *default* circuits.

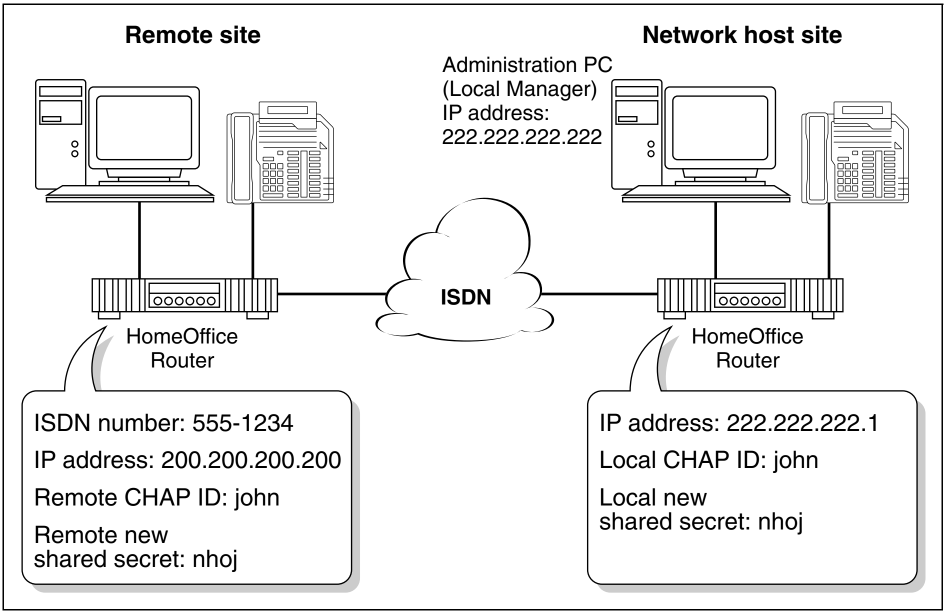
If it becomes necessary to have the capability to perform administration on more than 14 remote units, you can do one or both of the following:

- For each remote Router, create a backup of the administration configuration containing the access circuit for the specific remote site. The backup configuration file is given a name specific to that site (for example, JohnSmith_unit) and is restored to the administration Router when you need to upgrade or troubleshoot the telecommuter's Router.
- Use a load-balancing approach to divide the remote administration tasks and associated circuits for telecommuters between two or more administration Routers.

Configuration overview

1. Create an incoming circuit on the telecommuter's Router (see page 126).
2. Create a static route associated with the circuit on the telecommuter's Router (see page 131).
3. Create an outgoing circuit on the administration Router (see page 132).
4. Create a static route associated with the circuit on the administration Router (see page 137).

Configuration sample



Where to get more information

For circuit configuration and IP routes field descriptions, see the following:

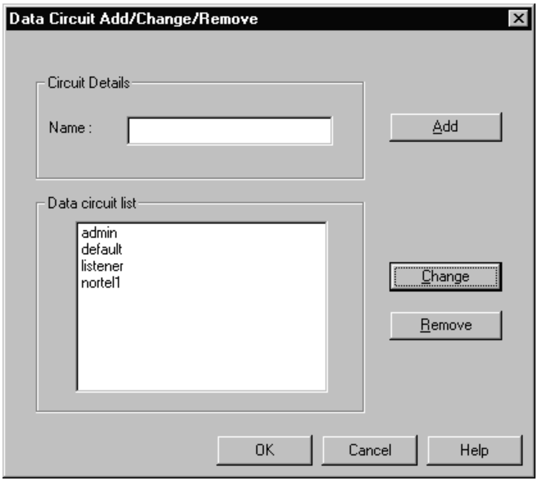
- "Data circuit configuration reference" on page 139
- "To create IP routes" on page 217

To create the circuit on the telecommuter's Router

1 Click the ISDN icon.

2 Select Circuits from the pop-up menu that appears.

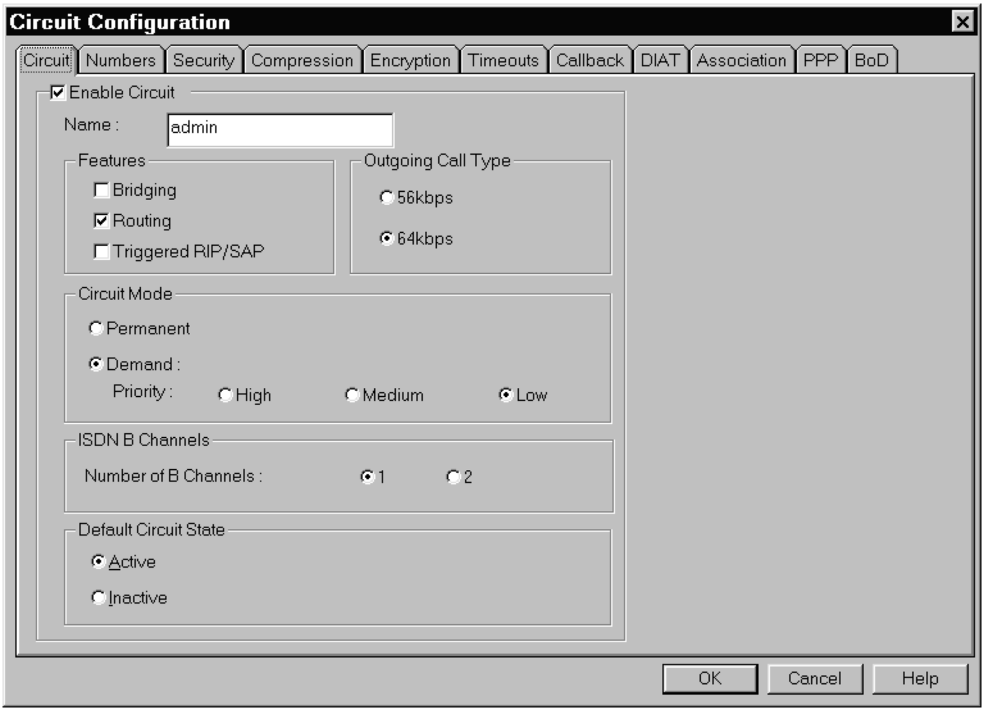
Result: The Data Circuit Add/Change/Remove screen appears.



admin
default
listener
nortel1

3 Select the admin circuit, and then click Change.

Result: The Circuit Configuration screen appears.



☑ Enable Circuit

Name : admin

Features

☐ Bridging

☑ Routing

☐ Triggered RIP/SAP

Outgoing Call Type

○ 56kbps

● 64kbps

Circuit Mode

○ Permanent

● Demand :

Priority : ○ High ○ Medium ● Low

ISDN B Channels

Number of B Channels : ● 1 ○ 2

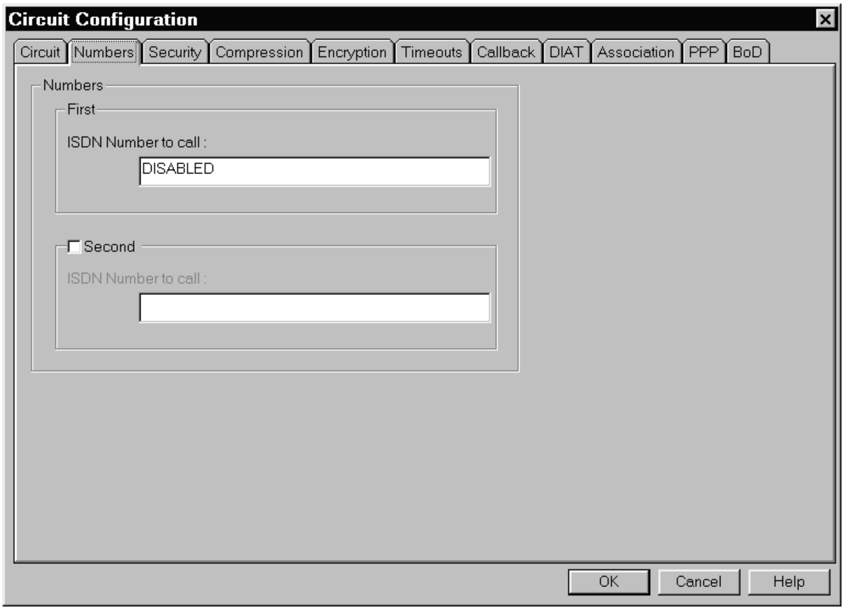
Default Circuit State

● Active

○ Inactive

4 Click the Numbers tab.

Result: The Numbers tab appears.



Numbers

First

ISDN Number to call : DISABLED

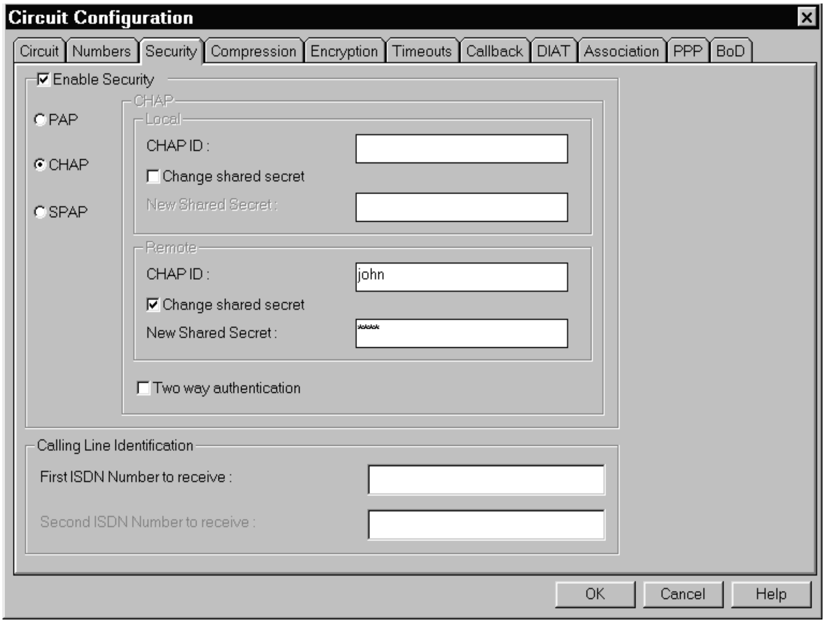
□ Second

ISDN Number to call :

5 Verify that the word DISABLED is shown in the ISDN Number to call box.

6 Click the Security tab.

Result: The Security tab appears.



☑ Enable Security

○ PAP

● CHAP

○ SPAP

CHAP

Local

CHAP ID :

□ Change shared secret

New Shared Secret :

Remote

CHAP ID : john

☑ Change shared secret

New Shared Secret : ****

□ Two way authentication

Calling Line Identification

First ISDN Number to receive :

Second ISDN Number to receive :

7 Ensure that the Enable Security check box is checked.

Result: The security configuration fields are enabled.

8 Select CHAP as the security method.

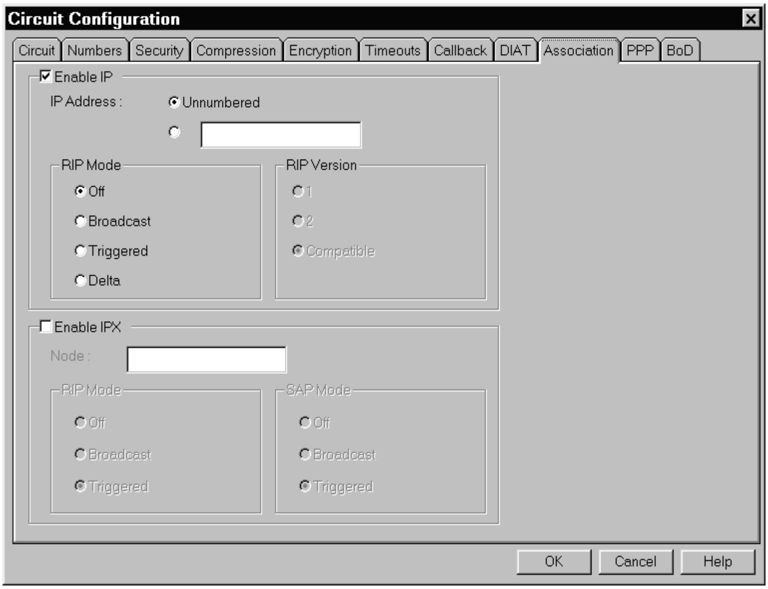
Result: The CHAP fields appear.

9 In the remote fields, enter the ID and password of the network administration Router.

Note: To enter the password, check the Change shared secret check box.

10 Click the Association tab.

Result: The Association tab appears.



☑ Enable IP

IP Address : ● Unnumbered

○

RIP Mode

● Off

○ Broadcast

○ Triggered

○ Delta

RIP Version

○ 1

○ 2

● Compatible

☐ Enable IPX

Node :

RIP Mode

○ Off

○ Broadcast

● Triggered

SAP Mode

○ Off

○ Broadcast

● Triggered

11 Click Enable IP.

12 Ensure that RIP Mode Off is selected.

13 Click OK.

Result: The Data Circuit Add/Change/Remove screen appears.

14 Click OK again.

Result: You return to the Local Manager Configuration tab.

15 Continue with “To create the static route on the telecommuter’s Router” below.

To create the static route on the telecommuter’s Router

1 Click the Admin icon.

2 Select IP Properties from the pop-up menu that appears.

Result: The IP Routes screen appears.

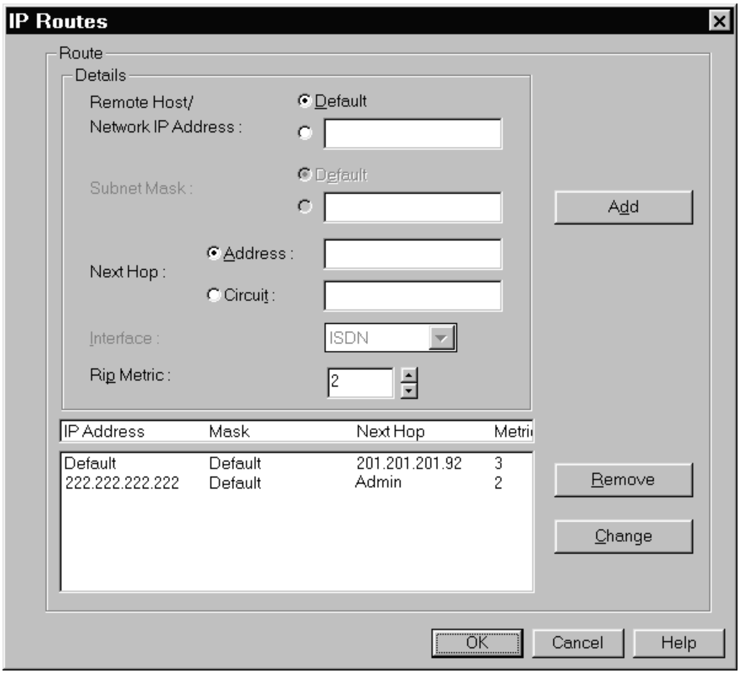
3 Enter the IP address of the network administration PC (not the network administration Router).

4 Click Default for the subnet mask.

5 Click Circuit, and then type the word “admin” (the name of the incoming circuit) into the Next Hop Circuit box.

6 Click Add.

Result: The new route appears in the table at the bottom of the screen.



IP Routes

Remote Host/ Network IP Address : ● Default ○

Subnet Mask : ● Default ○

Next Hop : ● Address : ○ Circuit :

Interface : ISDN

Rip Metric : 2

IP Address	Mask	Next Hop	Metri
Default	Default	201.201.201.92	3
222.222.222.222	Default	Admin	2

7 Click OK.

Result: You return to the Local Manager Configuration tab.

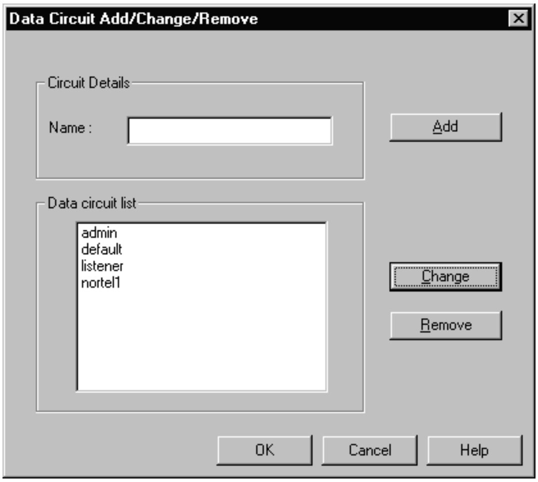
8 Continue with “To create the circuit on the administration Router” on page 132.

To create the circuit on the administration Router

1 Click the ISDN icon.

2 Select Circuits from the pop-up menu that appears.

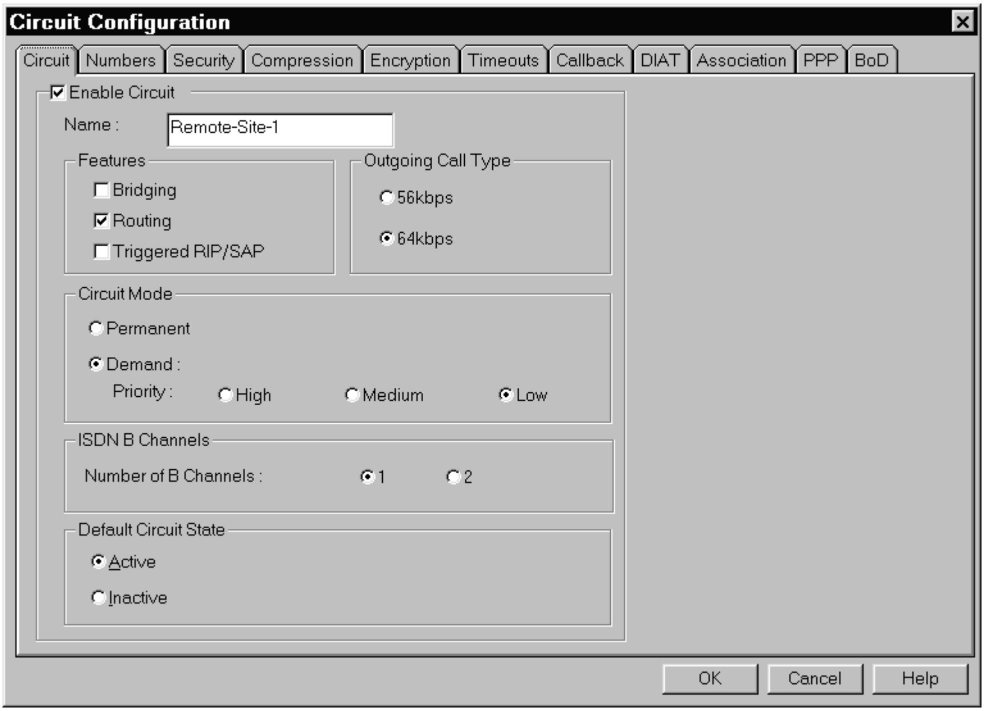
Result: The Data Circuit Add/Change/Remove screen appears.



3 Enter a name for the new circuit, and then click Add.

Note: The name should easily identify the remote site to which this circuit will connect.

Result: The Circuit Configuration screen appears.



Circuit Configuration

☑ Enable Circuit

Name : Remote-Site-1

Features

□ Bridging

☑ Routing

□ Triggered RIP/SAP

Outgoing Call Type

○ 56kbps

● 64kbps

Circuit Mode

○ Permanent

● Demand :

Priority : ○ High ○ Medium ● Low

ISDN B Channels

Number of B Channels : ● 1 ○ 2

Default Circuit State

● Active

○ Inactive

4 Click the Numbers tab.

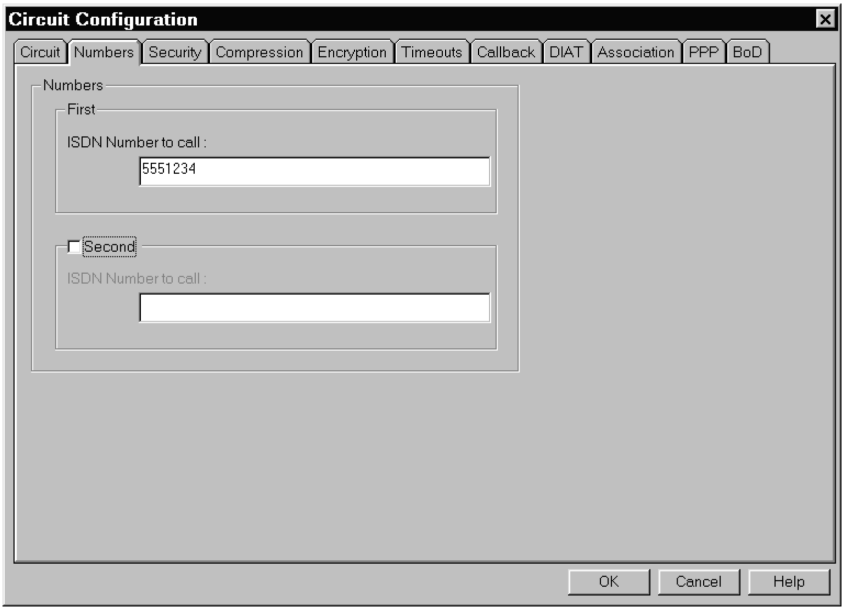
Result: The Numbers tab appears.

5 Type the telecommuter’s ISDN number into the First ISDN Number to call box.

Notes:

- You need only one B-channel on the circuit.
- Ensure that the ISDN number that you enter contains any dialing prefixes required to reach the remote site.

See the following example.



Numbers

First

ISDN Number to call : 5551234

☐ Second

ISDN Number to call :

6 Click the Security tab.

Result: The Security tab appears.

7 Click Enable Security.

Result: The security configuration fields are enabled.

8 Select CHAP as the security method.

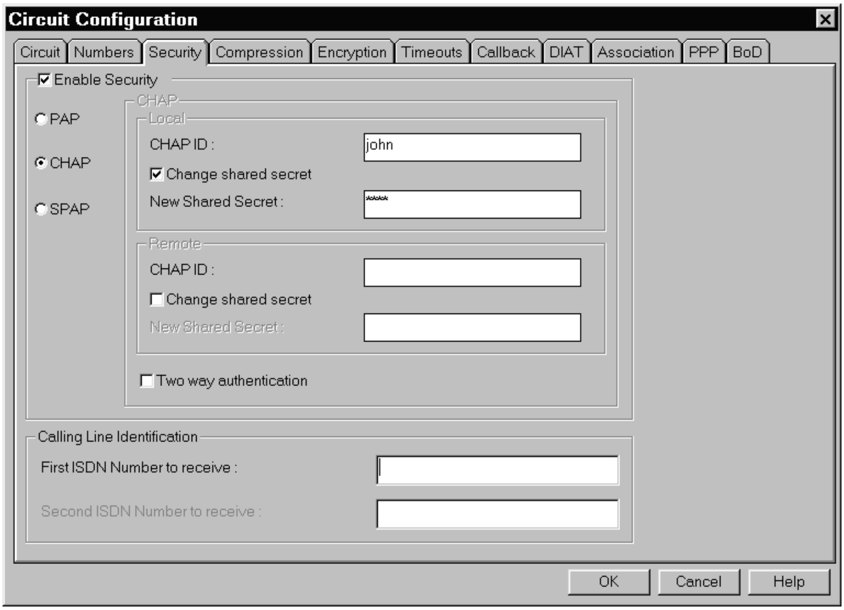
Result: The CHAP fields appear.

9 In the local fields, enter the ID and password of the network administration Router.

Notes:

- Enter the same user ID and password that you entered into the Remote fields on the telecommuter’s Router.
- To enter the password, check the Change shared secret check box.

See the following example.



☑ Enable Security

○ PAP

● CHAP

○ SPAP

CHAP ID : john

☑ Change shared secret

New Shared Secret : ****

CHAP ID :

□ Change shared secret

New Shared Secret :

□ Two way authentication

First ISDN Number to receive :

Second ISDN Number to receive :

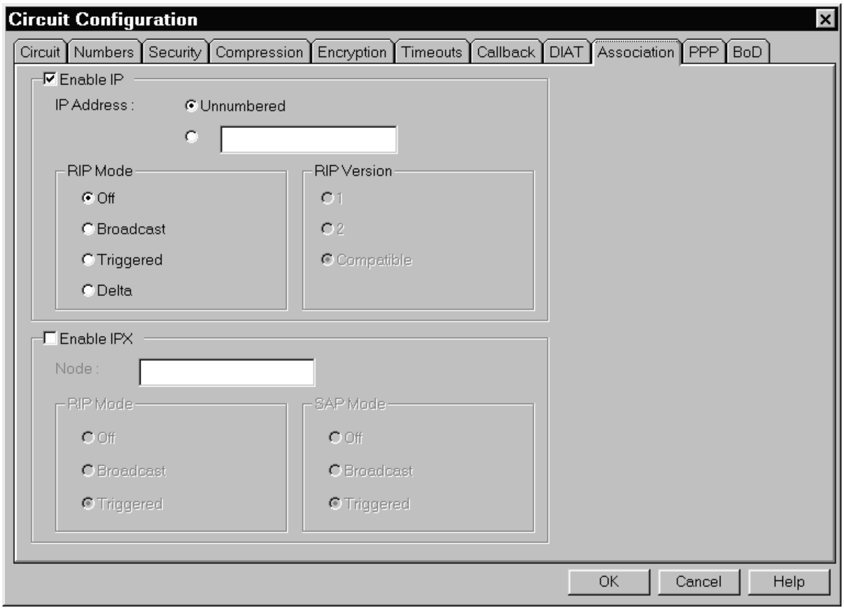
10 Click the Association tab.

Result: The Association tab appears.

11 Click Enable IP.

12 Ensure that RIP Mode Off is selected.

See the following example.



☑ Enable IP

IP Address : ● Unnumbered ○

RIP Mode: ● Off ○ Broadcast ○ Triggered ○ Delta

RIP Version: ○ 1 ○ 2 ● Compatible

□ Enable IPX

Node :

RIP Mode: ○ Off ○ Broadcast ● Triggered

SAP Mode: ○ Off ○ Broadcast ● Triggered

13 Click OK.

Result: The Data Circuit Add/Change/Remove screen appears.

14 Click OK again.

Result: You return to the Local Manager Configuration tab.

15 Continue with “To create the static route on the administration Router” below.

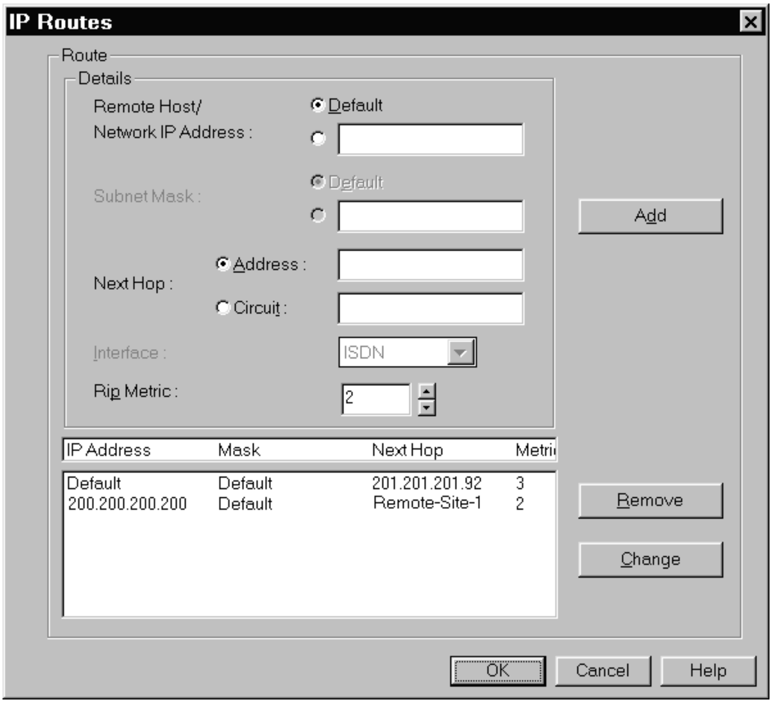
To create the static route on the administration Router

1. Click the Admin icon.
2. Select IP Properties from the pop-up menu that appears.

   Result: The IP Routes screen appears.
3. Enter the IP address of the telecommuter's Router.
4. Click Default for the subnet mask.
5. Click Circuit, and then enter the name of the outgoing circuit into the Next Hop Circuit box (see step 3 on page 132).
6. Click Add.

   Result: The new route appears in the table at the bottom of the screen.

   See the following example.



Remote Host/ Network IP Address : ● Default ○

Subnet Mask : ● Default ○

Next Hop : ● Address : ○ Circuit :

Interface : ISDN

Rip Metric : 2

IP Address	Mask	Next Hop	Metri
Default	Default	201.201.201.92	3
200.200.200.200	Default	Remote-Site-1	2

7. Click OK.

   Result: You return to the Local Manager Configuration tab.

What’s next?

Once you have configured both the administration and telecommuter Routers for remote access ISDN connections, you can establish a connection between them.

For instructions, see “Establishing a remote LAN-to-LAN connection” on page 355.

Section C: Data circuit configuration reference

In this section

Overview

Introduction

Use circuits to establish connections with remote sites, or to accept incoming calls from remote sites.

The circuit configuration consists of 11 screens as described in this section. You use most of these screens only to fine-tune a circuit.

Circuit tab

Use the Circuit tab to configure the following:

- circuit mode (demand or permanent)
- number of B-channels used
- default circuit state (active or inactive)
- protocols used

Numbers tab

Use the Numbers tab to configure the ISDN telephone numbers to call on outgoing circuits. On incoming circuits, set the ISDN telephone number to DISABLED.

Security tab

Most remote networks require some authenticating information before you can establish a connection. Authentication usually involves a user name and password that can be sent using a variety of authentication protocols.

The Router must have at least one form of security running to permit access to the telecommuter’s LAN. Use the Security tab to configure the following:

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)

- Shiva Proprietary Authentication Protocol (SPAP)
- Caller Line Identification (CLI)

Compression tab

Data compression is available for traffic over the ISDN link and is configured on the Compression tab. By compressing data, you can

- reduce transmission costs

  You can transfer more data across an existing link. Therefore, you do not need to pay for faster links.
- speed up communication

  The faster transfer of data helps telecommuters, while shorter ISDN calls also mean reduced costs.

Encryption tab

The encryption feature is currently unavailable and, therefore, cannot be configured.

Timeouts tab

On the Timeouts tab, you can define call duration, idle, and preemption timers for ISDN circuits that are configured as demand circuits. They are not required for permanent circuits.

Callback tab

The Callback tab allows you to configure callback (sometimes called dial-back) on ISDN circuits. This cost-saving feature allows you to take advantage of lower tariffs (where there is a discrepancy in the tariffs charged by the source and destination service providers).

To request callback, the Router must be

- connecting to a remote access switch that supports callback
- using SPAP authentication

DIAT tab

Dynamic IP or IPX Address Translation (DIAT) is a unique set of technologies for simplifying deployment of the HomeOffice Router and providing effective and secure network access. A single address represents the entire home or small office network. All of the devices on the HomeOffice Router's LAN share one address.

Note: DIAT is a form of Network Address Translation (NAT).

By default, DIAT for IP and IPX are disabled. You can enable DIAT for IP or IPX networking at any time, for either a single computer or multiple computers on the Router's network.

Association tab

The Association tab allows you to associate the destination address of the next hop routing device with the name of the circuit. You can enter one or both of the following:

- an IP address for IP circuits
- an IPX Node address for IPX circuits

PPP tab

Use the PPP tab to configure PPP timers. PPP timers make checks on the time taken to negotiate links between devices.

Note: In normal circumstances, you do not need to change the PPP timer values, as they are the default values for any router using the standard PPP setup. It is important that they are identical in both the original and target routers.

BoD tab

The Router allows the ISDN interface to temporarily provide additional bandwidth by using more virtual circuits when available. This is known as Bandwidth On Demand. Bandwidth on Demand is only available when the digital telephone is in offline mode.

The Bandwidth on Demand (BoD) tab allows you to do the following:

- Set up two or more ISDN B-channels to provide more bandwidth.

  This is known as Aggregation and is done using PPP Multilink.
- Set thresholds for increasing bandwidth.

  These thresholds determine when additional virtual circuits are opened.

Circuit tab

Introduction

Use the Circuit tab to configure the following:

- circuit mode (demand or permanent)
- number of B-channels used
- default circuit state (active or inactive)
- protocols used

Circuit modes

If you are using a demand ISDN circuit between HomeOffice Router and a remote access switch, you are only prompted for authentication information the first time the circuit is used. This can lead to reduced security.

If you have set the circuit mode to permanent, the circuit remains active until you deactivate it using Local Manager. You are prompted again for authentication the next time you reactivate the circuit.

Note: If the circuit goes down due to an idle timeout, you do not need to reauthenticate the next time the circuit comes back up. However, if you deactivate the circuit using Local Manager or the deactivate command, you must reauthenticate the next time you use the circuit.

For a higher level of security, you should set the circuit mode to permanent and the circuit state to inactive, which requires that you reactivate and reauthenticate each time you want to use the circuit. You should also deactivate the circuit when you finish using it.

If all resources are in use, a call can preempt another call that has a lower priority. If there is more than one call with the same priority, the call with the timer closest to expiring is preempted.

Number of B-channels

By default, one B-channel is enabled on HomeOffice Router.

By selecting two B-channels, you can place two data calls to a destination at the same time while in the offline mode to double the available bandwidth. However, if you do this, call prioritization may not work as described below.

When you use two B-channels, the following applies:

- Your ISDN bills are larger because you pay a separate call charge for each B-channel that you use, even if they are both calling the same number.
- The connection works only if the site dialed by the Router is provisioned to let you use both B-channels simultaneously.
- Your second B-channel is not active all of the time, but is brought up and taken down according to the amount of data being transferred.

  You can configure how often the line is brought up and down by setting the Bandwidth On Demand thresholds on the BoD tab. If you want to keep two B-channels open most of the time, set these thresholds to a minimum.

Call prioritization

When you are using one B-channel per destination, a call can only preempt another if it has a higher priority.

Outgoing calls can preempt one circuit at a time. If all available logical channels are in use, incoming voice calls can only preempt data calls if Additional Call Offering (ACO) is enabled and the data call is of a lower priority. Use the ISDN Interface tab in ISDN Properties to enable or disable ACO.

Circuit state

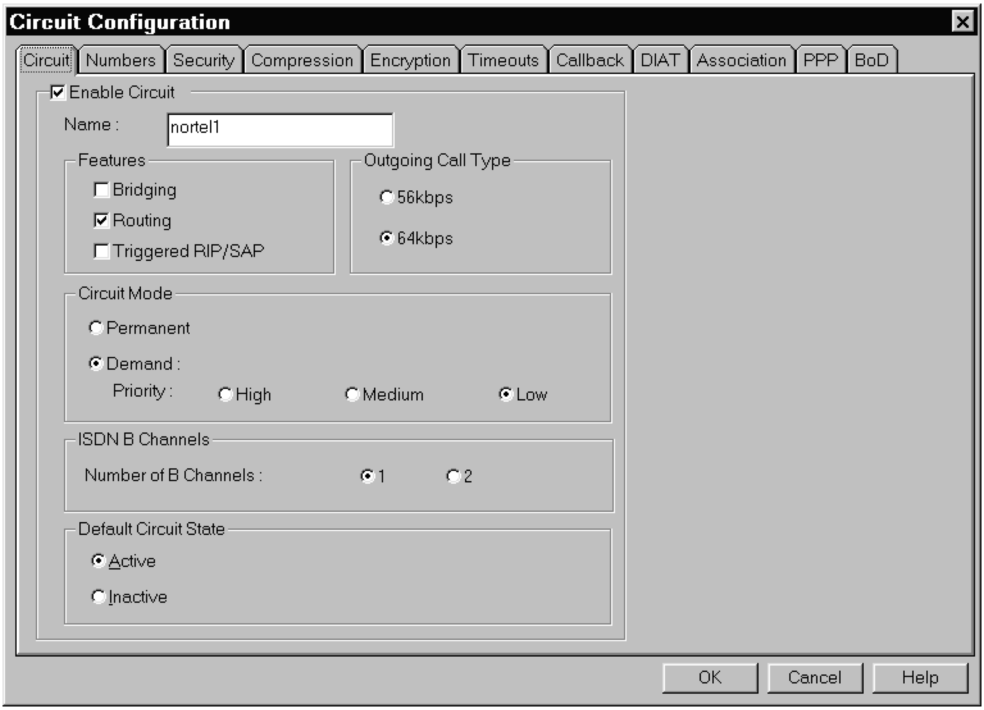
Each circuit on the HomeOffice Router has a default active or inactive state. This is the state that is resumed if you reboot the HomeOffice Router and interim configuration is lost. If the telecommuter connects to a network using a security server, set the circuit default state to inactive. You can then activate or deactivate each circuit individually using the Security option on the Edit menu in Local Manager.

To display the Circuit tab

1. Click the ISDN icon.
2. Select Circuits from the pop-up menu that appears.

   Result: The Data Circuit Add/Change/Remove screen appears.
3. Do one of the following:
   - Enter a name for the new circuit, and then click Add.
   - Select an existing circuit, and then click Change.

   Result: The Circuit Configuration screen appears.



☑ Enable Circuit

Name : nortel1

Features
- ☐ Bridging
- ☑ Routing
- ☐ Triggered RIP/SAP

Outgoing Call Type
- ○ 56kbps
- ● 64kbps

Circuit Mode
- ○ Permanent
- ● Demand :

  Priority : ○ High ○ Medium ● Low

ISDN B Channels

Number of B Channels : ● 1 ○ 2

Default Circuit State
- ● Active
- ○ Inactive

Circuit tab field descriptions

Field	Description
Enable Circuit	Click this check box if you want this circuit to be enabled immediately. Otherwise, leave it blank. The default is Enabled.
Name	Displays the name of the circuit that you are modifying.
Bridging	Click this check box if you want to bridge over this interface.
Routing	Click this check box if you want to route over this circuit.
Triggered RIP/SAP	Click this check box if you want to enable Triggered RIP and SAP on your circuit. **Notes:** • You must enable Triggered RIP and SAP when multiple static routes are being used. • If you are connecting the Router to an Intel Shiva LanRover Access Switch over IPX, you must select Broadcast RIP and SAP. Otherwise, select Delta RIP. Do this on the Circuit Configuration Association tab.
Outgoing Call Type	Select either 56 Kbps or 64 Kbps to indicate the speed of your ISDN line.
Permanent	Click Permanent if you are connecting to over IPX or if you have arranged with your service provider to be on an appropriate ISDN tariff. Permanent keeps the link open all of the time and prevents it from being preempted.
Demand	Click Demand to keep ISDN costs as low as possible. By selecting Demand, you can define whether calls on this circuit have a HIGH, MEDIUM, or LOW priority.

Field	Description
Number of B Channels	Select the number of B-channels that are available for transferring data on this circuit. You can enable one or two B-channels. If you enable two B-channels, your Router uses PPP Multilink on this circuit.
Default Circuit State	Select Active or Inactive as appropriate.

Numbers tab

Introduction

Use the Numbers tab to configure the ISDN telephone numbers to call.

International calls over ISDN

If you intend to make ISDN calls from North America, the United Kingdom, and France, or to Germany, you must note the following when you are configuring the HomeOffice Router's ISDN circuit table.

International dialing from North America

To make ISDN calls from North America to another country, you should proceed as if you were making an ordinary telephone call. You do not need to add any extra digits. The same applies if you are dialing from one state or province to another in North America.

International dialing from the United Kingdom

To make calls from the United Kingdom to another country, you must add an extra zero before the country code to tell the International Gateway that you are making an ISDN call. For example, if you want to call a bridge in Paris with the address (1) 44110055, you must dial 00033144110055. The parts of this number break down as follows:

00	0	33	1	44110055
International code	Extra zero	Country code	Area code	ISDN number

International dialing from France

If you want to make calls from France to another country, you need to add 09 before the country code. For example, to call Edinburgh (0131) 9985443 from France, you must dial 0009441319985443. The parts of this number break down as follows:

00	09	44	131	9985443
International code	Extra digits	Country code	Area code	ISDN number

International dialing to Germany

When initiating a data connection to Germany, you must add an extra zero before the country code (from the United Kingdom only) and another zero at the end of the ISDN address (from all countries). For example, to call Bonn (0228) 9868006 from the United Kingdom, you must dial 0004922898680060. The parts of this number break down as follows:

00	0	49	228	9868006	0
International code	Extra zero (from the United Kingdom only)	Country code	Area code	ISDN number	Extra zero

Specifying the ISDN number for an incoming circuit

If you want your Router to receive incoming calls only (for example, if it is located at head office and receives calls from remote offices), you can type the word DISABLED into the ISDN Number to Call field. If your Router has DISABLED entered as the number to call, then it cannot use the circuit to make outgoing calls.

To display the Numbers tab

1. Click the ISDN icon.
2. Select Circuits from the pop-up menu that appears.

   Result: The Data Circuit Add/Change/Remove screen appears.

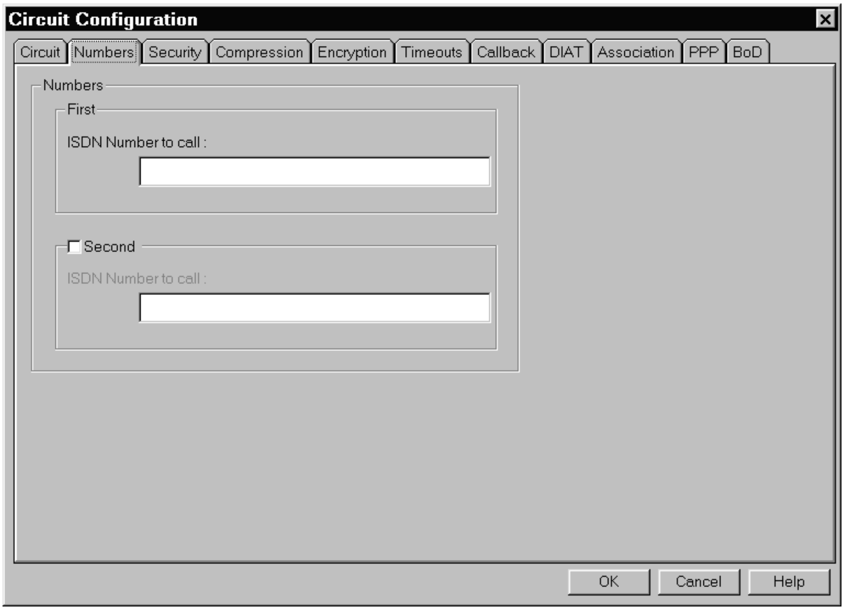
3 Do one of the following:

- Enter a name for the new circuit, and then click Add.
- Select an existing circuit, and then click Change.

Result: The Circuit Configuration screen appears.

4 Click the Numbers tab.

Result: The Numbers tab appears.



Circuit Configuration

Numbers

First

ISDN Number to call :

□ Second

ISDN Number to call :

Numbers tab field descriptions

Field	Description
First ISDN Number to call	• For outgoing calls: Enter the ISDN phone number that the Router should use when making an outgoing call to a remote destination. This can be up to 41 digits in length. Ensure that you include any necessary codes. If you enter an area code, ensure that you type it directly before the main telephone number (for example, 6173312561). Do not type a hyphen after the area code (-). Hyphens are reserved for sub-addressing. • For incoming calls: If this circuit is to be used for incoming calls only, type the word DISABLED.
Second	If the remote device' ISDN variant is NI-1, you must enter a second ISDN phone number to make calls over both B-channels. Click this check box to enable the second ISDN Number to Call field.
Second ISDN Number to Call	See First ISDN Number to call. Only include the remote sub-address if the switch forwards the calling sub-address.

Security tab

Introduction

Most remote networks require some authenticating information before a connection can be established. Authentication usually involves a name and password that can be sent using a variety of authentication protocols.

The Router must have at least one form of security running; otherwise, it cannot receive any calls. Configure the security method on the Security tab.

Security authentication methods

The HomeOffice Router supports three types of password authentication:

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Shiva Password Authentication Protocol (SPAP)

Some incoming calls may not include the Caller ID. Similarly, the Router's Caller ID may not be passed to a device that it is calling. This can occur when you make international calls or when Caller ID is unavailable and can mean reduced security.

When these circumstances apply, you can choose PAP, CHAP, or SPAP to add an extra level of security on the ISDN link. CHAP and SPAP are the most secure methods because they use encryption to transfer passwords.

Note: If the telecommuter needs to receive incoming calls but does not have Caller ID, you must enable PAP, CHAP, or SPAP.

Password Authentication Protocol

As a part of the PPP suite, PAP is a protocol that provides additional network security on PPP links. It enables login IDs and passwords to be transmitted over the link so that a remote device can authenticate the telecommuters.

PAP is not very secure because it sends the password in plain text across the link.

Challenge Handshake Authentication Protocol

Also a part of the PPP suite, CHAP is an authentication protocol that provides additional network security so that a remote access device can authenticate the telecommuters. CHAP is secure because it uses a cryptographic handshake to transmit and receive password information.

Shiva Password Authentication Protocol

Shiva Password Authentication Protocol (SPAP) is a proprietary security authentication mechanism for PPP negotiation with Intel Shiva LanRover Access Switches.

SPAP is configurable for all circuits, including the listener and default circuits, on a circuit-by-circuit basis. SPAP (like PAP and CHAP) allows you to interoperate between a HomeOffice Router and an Intel Shiva LanRover Access Switch.

There are two main uses for SPAP:

- authentication
- additional functionality for interoperating with other devices

In addition, SPAP offers the following enhanced functionality:

- dial-on-demand
- third-party security (such as SecurID/AssureNet Pathways support)

SPAP passwords are encrypted, meaning increased security.

Caller ID

Caller ID or Calling Line Identification (CLI) is a mechanism for identifying incoming calls. You may be able to order Caller ID from your ISDN service provider as part of the ISDN service.

The Router stores *ISDN Address received* entries in its circuit table and checks incoming calls against these addresses. You can use this to add an extra level of security.

SPAP and return calling number

If this circuit is a demand circuit, you must enter a return ISDN phone number so the network host site can call the Router when the link goes down.

If you do not enter a number, you cannot monitor the HomeOffice Router remotely using an Intel Shiva LanRover Access Switch. However, if you do enter a number, the telecommuter may receive some unwanted calls, which occur because certain network monitoring applications periodically send packets to check that the HomeOffice Router is responding.

If this circuit is a permanent circuit, you do not need to enter a return ISDN telephone number because the link never goes down.

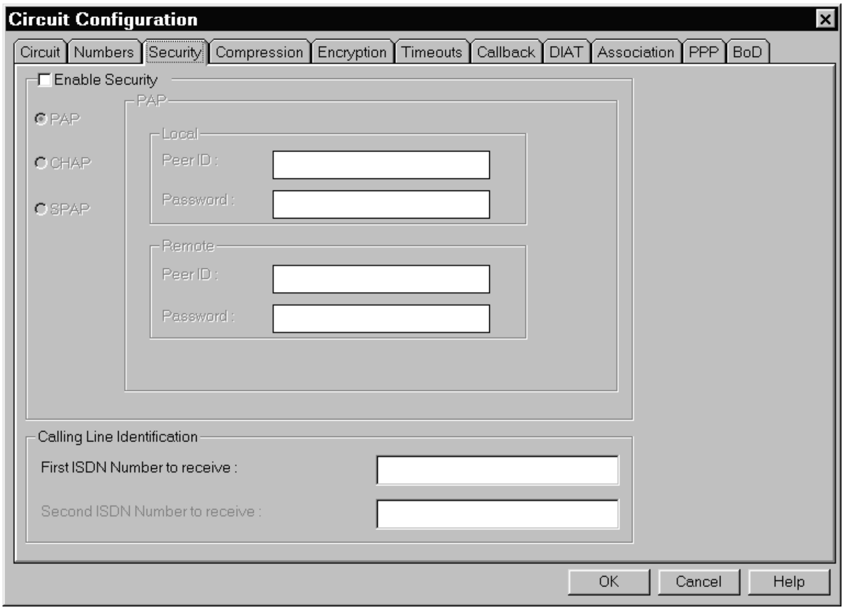
To display the Security tab

1. Click the ISDN icon.
2. Select Circuits from the pop-up menu that appears.

   Result: The Data Circuit Add/Change/Remove screen appears.
3. Do one of the following:
   - Enter a name for the new circuit, and then click Add.
   - Select an existing circuit, and then click Change.

   Result: The Circuit Configuration screen appears.
4. Click the Security tab.

   Result: The Security tab appears.



Security tab field descriptions

Field	Description
Enable Security	To use Caller ID only as the security method, ensure that this check box is blank. (If you do this, you must enter a Caller ID [CLI] number in the ISDN Number to receive fields.) To enable security, click this check box. The PAP, CHAP, and SPAP buttons are activated. If Callback will be used, you must select PPP as the Callback ID in the Callback tab for PAP, CHAP, and SPAP to work when making an outgoing call.
Security type	Click the security authentication method being used by your network. The appropriate fields appear for PAP, CHAP, or SPAP.

Field	Description
Fields for PAP	
Local Peer ID	This is the identifier for the Router. The Peer ID identifies the Router when it makes an outgoing call. Enter a Peer ID of up to 48 characters. As an example, you could use the Router's ISDN address or location name. Ensure that the Router's Peer ID and Password are the same as the Peer ID and Password that have been set up on the remote access switch.
Local Password	The PAP password works in conjunction with the Peer ID. Enter a password of up to 15 characters. **Note:** To be effective, the password should be different from the Peer ID.
Remote Peer ID	**Note:** This field is optional. This is the identifier for the remote device. Enter the Peer ID of up to 48 characters for the remote device. When an incoming call is received by the Router, the Router uses this field to verify the Peer ID of the remote device. **Notes:** • Ensure that the remote Peer ID is unique. Otherwise, it will not be registered. • The same parameter values must be defined in reverse on the device at the other end of the circuit.
Remote Password	**Note:** This field is optional. Enter the PAP password of up to 15 characters for the remote device. When an incoming call is received, the Router uses this field to verify the PAP password of the remote device.

Field	Description
Fields for CHAP	
Local CHAP ID	Enter the Router’s CHAP ID of up to 48 characters. This identifies the Router when making outgoing calls.
Change shared secret (local)	Check this check box if you want to enter a new shared secret or change an already configured shared secret.
New shared secret (local)	Enter a password of up to 25 characters for the Router. This password is sent on the link from the Router to the device at the other end of the circuit when attempting to establish a call. **Note:** The shared secret should be different from the CHAP ID.
Remote CHAP ID	**Note:** This field is optional. Enter a unique CHAP ID for the device at the other end of the circuit. This identifies the remote site when the Router receives an incoming call. Type the word NONE if the Router can only dial out on this circuit.
Change shared secret (remote)	Check this check box if you want to enter a new shared secret or change an already configured shared secret.
New shared secret (remote)	Enter a password of up to 25 characters for the device at the other end of the circuit. The device at the other end of the link should be configured to send this password when it attempts to establish a call to the Router.
Two-way authentication	Click this check box to enable two-way authentication. This allows devices at either end of the link that are running CHAP to authenticate each other simultaneously.

Field	Description
Fields for SPAP	
Return Phone Number	**Note:** This field is optional. If you are configuring this circuit as a demand circuit, enter the Router's ISDN telephone number (assigned to data). The device at the remote site uses this number to call this Router. The number can be up to 32 digits in length. Ensure that you include any necessary area dialing codes, such as 9 to use an outside line, 1 for long-distance calls, and so on. Otherwise, leave the field blank.
Local Peer ID	This identifies the Router when making outgoing calls. Enter a Peer ID of up to 48 characters (including any spaces) for the Router that you are configuring. Ensure that the Router Peer ID matches the user list entry that has been set up on the remote access switch.
Change password	Check this check box if you want to change an already configured password.
Password	**Note:** This field is optional. The password works in conjunction with the Peer ID. It is an additional identifier. Enter a password of up to 16 characters (including any spaces) for the Router. This password is encrypted and sent on the link from the Router to the device at the other end of the circuit when attempting to establish a call. Ensure that the Router password is the same as the password that has been set up on the Intel Shiva LanRover Access Switch.

Field	Description
Remote Peer ID	**Note:** This field is optional. This identifies the remote site when the Router receives a call. Enter the Intel Shiva LanRover Access Switch's Peer ID. The Peer ID can contain up to 48 characters, including any spaces.
Change password	Check this check box if you want to change an already configured password.
Password	Enter the password (up to 16 characters) that the Intel Shiva LanRover Access Switch at the other end of the circuit uses to authenticate itself when calling the Router. The Router checks the Peer ID and Password of the remote device to identify incoming callers. **Note:** The same parameter values must be defined in reverse on the Intel Shiva LanRover Access Switch at the other end of the circuit.
Fields for Calling Line Identification	
First ISDN Number to receive	Enter the ISDN number of the remote device. **Note:** If you want to disable Caller ID because you do not want to use it or the ISDN interface does not support it, leave this field blank.
Second ISDN Number to receive	If the remote device's ISDN variant is National ISDN-1, enter the second ISDN number of the remote device. This allows identification of calls on both B-channels.

Compression tab

Introduction

Data compression is available for traffic over the ISDN link. By compressing data, you can

- reduce transmission costs

  You can transfer more data across an existing link. Therefore, you do not need to pay for faster links.
- speed up communication

  The faster transfer of data helps telecommuters, while shorter ISDN calls also mean reduced costs.

PPP Multilink Protocol

The PPP Multilink Protocol (RFC 1717) is a standardized extension of the Point-to-Point Protocol (PPP) standard. It allows you to

- combine channels into a multilink bundle so that data can be sent at higher rates
- use packet sequencing to order packets
- ensure compatibility between manufacturers of internetworking equipment

You can also enable a feature known as packet fragmentation where larger individual packets are chopped into smaller fragments. This occurs during bandwidth aggregation. These fragments are then distributed among all of the channels in use. The receiver at the other end of the links collects the fragments, and then reassembles and delivers them in the original order.

You can use Local Manager to enable Multilink Compression. To fine-tune PPP Multilink, use the command shell.

Notes:

- Multilink compression only works if both ends of the link are set the same.

- You should have networking experience before fine-tuning PPP Multilink. Telecommuters who are configuring PPP Multilink to work on their Router should not perform any fine-tuning.

Before configuring PPP Multilink on the HomeOffice Router, you must ensure that you have configured two virtual circuits. These can be two ISDN B-channels.

PPP Multilink functions and features

PPP Multilink has the following functions:

- combining links into a multilink bundle
- packet sequencing and ordering
- packet fragmentation over a number of B-channels to reduce latency (this speeds up transmission)
- Address and Control Field Compression
- Protocol Field Compression

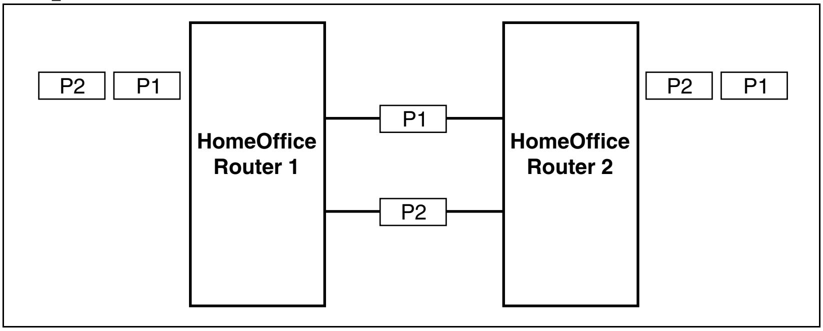
PPP Multilink is advantageous because it ensures packet ordering. It also guarantees compatibility with other vendors' equipment because it is an open standard. Packet fragmentation over a number of links is beneficial because it reduces latency (the length of time a packet waits to receive an acknowledgment from the other end of the link), which decreases transit times and, therefore, speeds up transmission.

Packet fragmentation

With PPP Multilink, you can enable packet fragmentation. The following illustrations show how packet fragmentation changes the way packets are transmitted between two Routers. When packet fragmentation is not enabled, packets are sent whole across the B-channels from Router 1 to Router 2.

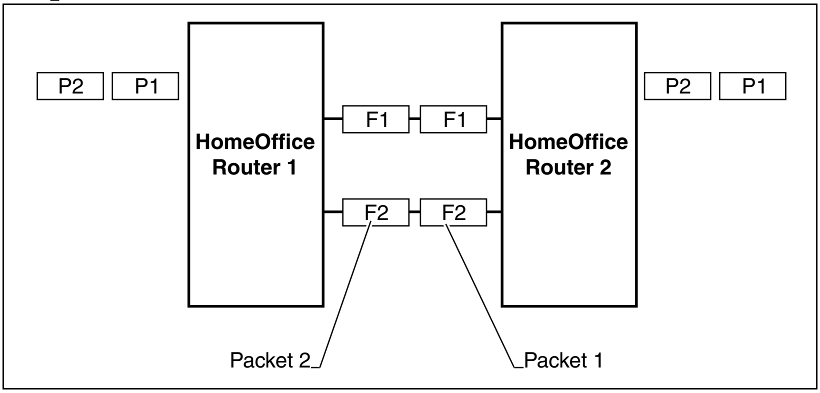
Packet transmission without fragmentation

ISG616_I



Packet transmission with fragmentation

ISG615_I



The larger packets are chopped into smaller fragments and distributed from Router 1 to Router 2 over all the channels in use. When you send them in this way, it reduces transit times. The receiver collects the fragments, reassembles them, and delivers them in the original intended order.

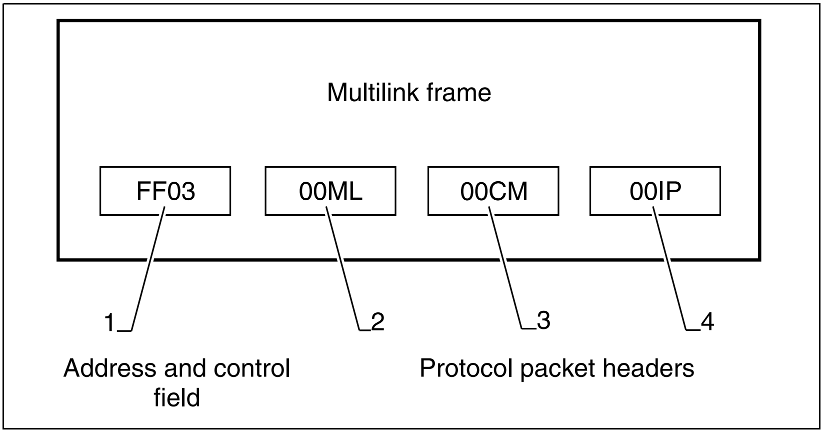
Compression

Link compression (sometimes called *compress after Multilink*) means that data compression occurs independently on each link of the Multilink bundle.

Bundle compression (sometimes called *compress before Multilink*) means that data compression occurs before the packets are split onto different links of the Multilink bundle. It provides a better compression ratio than link compression and should be used if you do not gain any performance advantage with link compression.

The following illustration shows how compression affects a multilink frame.

ISG110_D



If you enable Address and Control Field Compression, Field 1 of the frame is compressed. If you enable Protocol Field Compression on both units, and negotiation is successful, each protocol header (Fields 2, 3, and 4) is compressed, including the multilink header (2). Compression is advantageous because there are fewer octets to transmit.

To display the Compression tab

1 Click the ISDN icon.

2 Select Circuits from the pop-up menu that appears.

Result: The Data Circuit Add/Change/Remove screen appears.

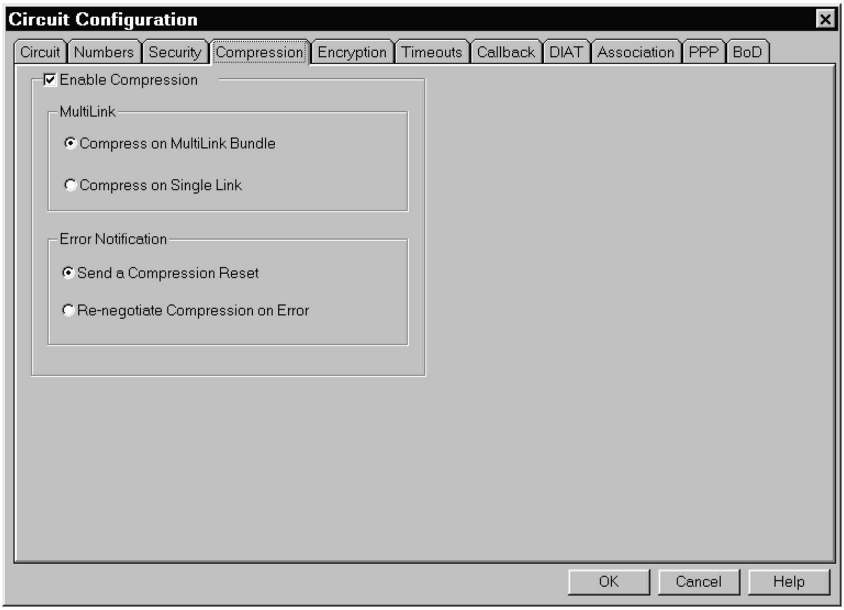
3 Do one of the following:

- Enter a name for the new circuit, and then click Add.
- Select an existing circuit, and then click Change.

Result: The Circuit Configuration screen appears.

4 Click the Security tab.

Result: The Compression tab appears.



☑ Enable Compression

MultiLink

● Compress on MultiLink Bundle

○ Compress on Single Link

Error Notification

● Send a Compression Reset

○ Re-negotiate Compression on Error

Compression tab field descriptions

Field	Description
Enable Compression	Click this check box to enable compression on the circuit that you are configuring. The Router negotiates a compression algorithm with the remote device each time it connects.
Compress on Multilink Bundle	Select this option if the Router is interoperating with a HomeOffice Router or another vendor's equipment.

Field	Description
Compress on Single Link	Select this option if the remote device's circuit is running over a device that performs compression on the front-end card. By choosing LINK, you can take advantage of the compression on the remote Primary Rate ISDN card. Compression on the card means that resources are freed up on the motherboard. This can result in improved overall throughput, despite the slightly less effective compression.
Send a Compression Reset	Select this option if you want the Router to notify the remote access switch that a compression error has occurred. **Note:** This is the default.
Re-Negotiate Compression on Error	Select this option if you know that the remote device uses Configuration-Request to notify the occurrence of a compression error.

Encryption tab

Introduction

The encryption feature is currently unavailable and, therefore, cannot be configured.

To display the Encryption tab

1 Click the ISDN icon.

2 Select Circuits from the pop-up menu that appears.

Result: The Data Circuit Add/Change/Remove screen appears.

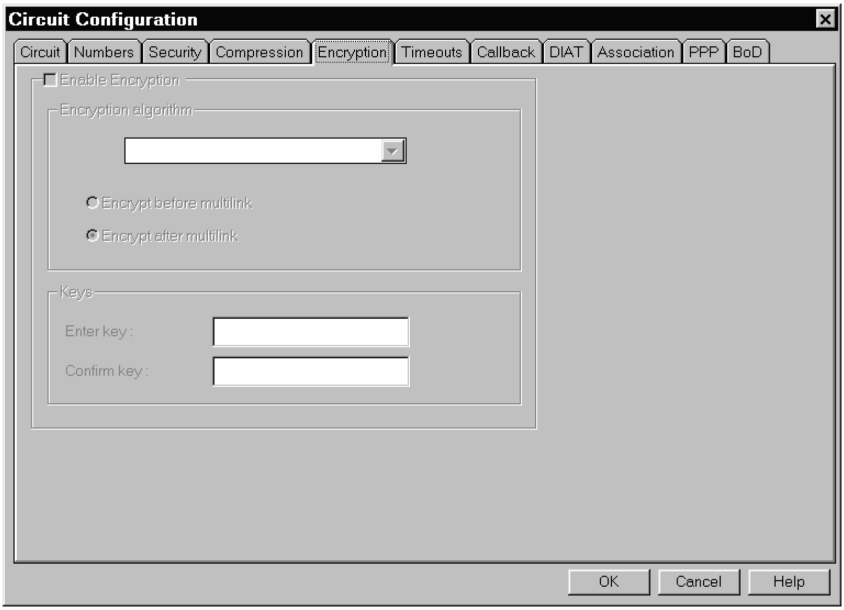
3 Do one of the following:

- Enter a name for the new circuit, and then click Add.
- Select an existing circuit, and then click Change.

Result: The Circuit Configuration screen appears.

4 Click the Encryption tab.

Result: The Encryption tab appears.



Circuit Configuration

□ Enable Encryption

Encryption algorithm

○ Encrypt before multilink

● Encrypt after multilink

Keys

Enter key :

Confirm key :

Timeouts tab

Introduction

On the Timeouts tab, you can define call duration, idle, and preemption timers for ISDN circuits that are configured as demand circuits. They are not required for permanent circuits.

Call duration timer

Most ISDN tariffs specify a minimum unit of time for which you are charged when you open a circuit, regardless of whether you use it for the full period of time. The call duration timer specifies the minimum length of time that each ISDN call remains open, regardless of data or telephone activity (or lack thereof). For example, if your ISDN service provider charges a minimum of 90 seconds and your call lasts only 20 seconds, a charge of 90 seconds is incurred.

If you make more calls during the 90-second time frame, a charge is incurred only for one ISDN call, because the original ISDN call has not yet been closed.

Idle timer

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

For example, if you set the idle timer to 60 seconds, the ISDN call remains open for 60 seconds after you hang up. Note that if you dial another number before 60 seconds have passed, you do not have to open another ISDN call.

Preemption timer

If all resources are in use, a call can preempt another call that has a lower priority. If there is more than one call with the same priority, the call with the timer closest to expiring is preempted.

When you are using one B-channel per destination, a call can only preempt another if it has a higher priority.

Outgoing calls can preempt one circuit at a time. If all of the available logical channels are in use, incoming voice calls can only preempt data calls if Additional Call Offering (ACO) is enabled and the data call is of a lower priority.

Note: ACO is enabled or disabled on the ISDN interface (ISDN Properties).

How the timers are defined

The call duration and idle timers are defined for ISDN circuits within Local Manager. If you want to use the HomeOffice Router command shell, you can configure the call duration timers using the `network isdn2 default` command, which allows you to set up a circuit configuration that applies to all of the new circuits created on a selected interface. The `network isdn2 tune` command changes circuit parameters on an individual basis.

To display the Timeouts tab

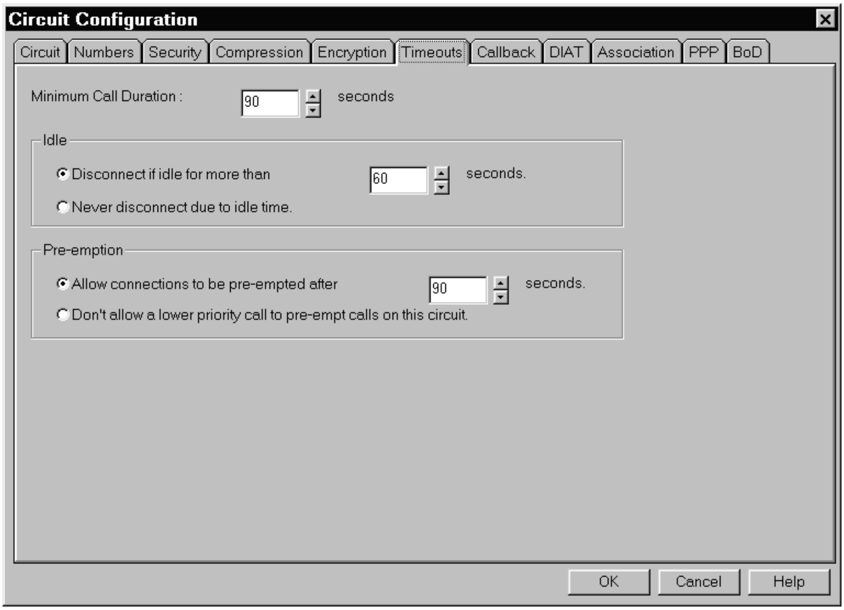
1. Click the ISDN icon.
2. Select Circuits from the pop-up menu that appears.

   Result: The Data Circuit Add/Change/Remove screen appears.
3. Do one of the following:
   - Enter a name for the new circuit, and then click Add.
   - Select an existing circuit, and then click Change.

   Result: The Circuit Configuration screen appears.

4 Click the Timeouts tab.

Result: The Timeouts tab appears.



Minimum Call Duration : 90 seconds

Idle

● Disconnect if idle for more than 60 seconds.

○ Never disconnect due to idle time.

Pre-emption

● Allow connections to be pre-empted after 90 seconds.

○ Don't allow a lower priority call to pre-empt calls on this circuit.

Timeouts tab field descriptions

Field	Description
Minimum Call Duration	Enter the minimum time in seconds that you want this circuit to remain open. Set a time between 0 and 3600 seconds. The default is 90. Enter a value that is slightly less than the length of time that corresponds to the minimum call charge set by the service provider. For example, if the service provider rounds up any call of less than one minute to charge for a full minute, enter a value of 59 seconds in this field. This means that the circuit is configured to remain open for at least the time for which you are paying.

Field	Description
Disconnect if idle for more than	Click this option if you want to define how long a connection can remain idle before closing. Then enter a number of seconds between 1 and 3600. The default is 60. **Note:** If you set the value too low, especially on links with long connection setup times, this can result in a connection always timing out before it is properly established.
Never disconnect due to idle time	Click this option if you do not want connections on this circuit to time out.
Allow connections to be preempted after	Click this option if you want to define how long a connection can be open before it can be preempted by another call. Then enter a number of seconds between 1 and 43 200. The default is 90. **Note:** This setting is ignored if the other call has a higher priority.
Don’t allow a lower priority call to preempt calls on this circuit	Select this option if you do not want connections to be preempted, other than by calls with higher priority.

Callback tab

Introduction

The Callback tab allows you to configure callback (sometimes called dial-back) on ISDN circuits. This cost-saving feature allows you to take advantage of lower tariffs (where there is a discrepancy in the tariffs charged by the source and destination service providers).

To request callback, the Router must be

- connecting to a remote access switch that supports callback
- using SPAP authentication

Types of Callback

Callback can be one of the following:

- fixed Caller ID
- roaming Caller ID
- PPP

Note: PPP must be running for callback to work when making a call, regardless of whether you choose Caller Line Identification or PPP.

Fixed Caller ID

Configure the HomeOffice Router's telephone number associated with the data port on the remote access switch.

If you choose fixed callback on the remote access switch, then you must choose SPAP as the authentication method for both the incoming and outgoing circuits for Callback to work.

Roaming Caller ID

Configure the HomeOffice Router's telephone number associated with the data port on the HomeOffice Router in the Return Phone Number field for SPAP on the Security tab.

If you choose roaming callback on the remote access switch, then you must choose SPAP as the authentication method on both the HomeOffice Router and the remote access switch.

PPP

Callback is based on PPP negotiation.

Note: If you use roaming callback with PPP, and the remote device is an Intel Shiva LanRover Access Switch, Microsoft's callback protocol (CBCP) should be disabled for the phone group on the Intel Shiva LanRover Access Switch.

If you choose PPP, then you must choose either PAP or CHAP as the authentication method for Callback to work.

How callback works

Callback is enabled on an interface and each circuit has the option to use it. You can configure a circuit to

- generate a Callback request
- accept a Callback request
- have Callback disabled

If configured to generate a Callback request, the Router generates an outgoing data call to a remote access switch. If the request is accepted by the remote access switch (that is, the user name and password presented to the remote access switch are correct and callback privileges are configured for the telecommuter), the call is dropped and the remote access switch calls the Router back.

If configured to accept a Callback request, the HomeOffice Router drops the incoming call after successfully authenticating the remote access switch, and calls the remote access switch back.

Note: The HomeOffice Router cannot accept callback requests from a remote Intel Shiva LanRover Access Switch.

How Callback with Caller ID (CLI) works

When a call arrives on a circuit that is configured to accept Callback requests, the HomeOffice Router rejects the incoming SETUP message and calls back the originator using the number presented by Caller ID. This method means that there is either no charge or a minimal call setup charge (service provider dependent) to the originator.

If the originator is not configured to request Callback but the receiving circuit is configured to call back the originator, then when a call arrives, the originator is still called back. This means that a small amount of data is lost since the originator did not request Callback and, therefore, did not queue any traffic. However, the end systems should be able to cope with this.

If the originator is configured to request Callback but the receiving end is not configured to call back, then the receiving end accepts the call and the originator pays the cost of the call.

How Callback with PPP works

A call is accepted by the listener circuit, and then Callback is negotiated using PPP as described in RFC 1750. With this method, a small cost is incurred at the originating end since the call has to be accepted before Callback is negotiated. If the negotiation fails, then the call proceeds with the originator paying the cost of the call.

On the unit receiving the call, you can configure a delay before returning the call. This is the length of time that you want to allow for incoming calls to be cleared before another call is accepted.

On the unit requesting Callback, you can configure the amount of time that the unit waits for the call to be returned.

Benefits of using Callback

You can use Callback for the following purposes:

- as a security feature
- to take advantage of any differences in call charges (where the service at each end of a link is provided by different service providers, who apply different tariffs)
- to provide centralized billing

To display the Callback tab

1 Click the ISDN icon.

2 Select Circuits from the pop-up menu that appears.

Result: The Data Circuit Add/Change/Remove screen appears.

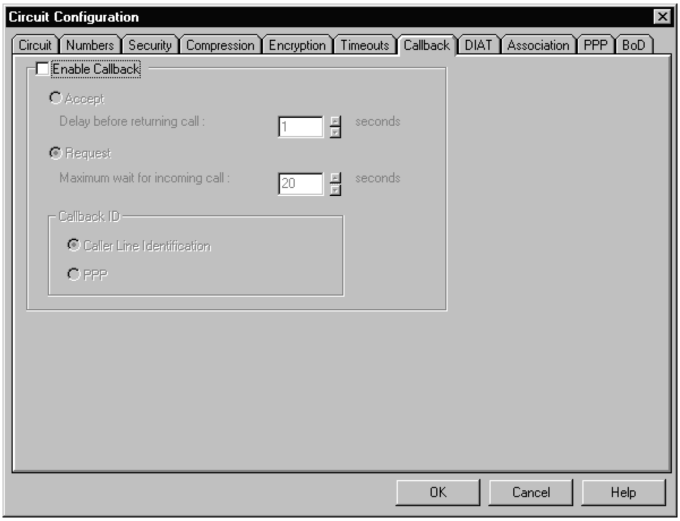
3 Do one of the following:

- Enter a name for the new circuit, and then click Add.
- Select an existing circuit, and then click Change.

Result: The Circuit Configuration screen appears.

4 Click the Callback tab.

Result: The Callback tab appears.



Circuit Configuration

□ Enable Callback

○ Accept

Delay before returning call : 1 seconds

● Request

Maximum wait for incoming call : 20 seconds

Callback ID

● Caller Line Identification

○ PPP

Callback tab field descriptions

Field	Description
Enable Callback	Click this check box to enable callback for this circuit.
Accept	Select this option if you want the HomeOffice Router to accept a callback request. When you select this option, the Delay before returning call field is activated.
Delay before returning call	Enter the length of time, between 1 and 60 seconds, that the HomeOffice Router should wait before making the return call. This allows time for clearing incoming calls. The default is 1. A value of around four seconds is recommended to allow for different switch types.
Request	Select this option if you want the HomeOffice Router to request a callback from the remote site using roaming dial-back. Be aware of the following if you are requesting callback: • The Router must be calling a remote access switch that supports callback and using SPAP authentication. • The associated account on the remote access switch must be configured for roaming dial-back. If the account is configured for required dial-back and you configure the Router to request dial-back, the call cannot be completed. When you select this option, the Maximum wait for incoming call field is activated.
Maximum wait for incoming call	Enter the maximum length of time, between 5 and 120 seconds, that the HomeOffice Router should wait before receiving the incoming call. The default is 20. Data is queued until the remote device returns the call or this period elapses.

Field	Description
Caller Line Identification	If you want to save money, select this option. It is generally cheaper to operate callback with Caller Line Identification (CLI) than with PPP. With CLI, the remote access switch rejects your initial call and immediately dials back the originating site (the Router's ISDN line). Most telephone companies do not charge for this initiating call.
PPP	Select this option if you know that Callback with CLI does not work with your remote access switch. PPP interoperates with most remote access products while Caller Line Identification (CLI, or Caller ID) may not. If you select this option, you must configure PAP, CHAP, or SPAP for callback to work. Use the Security tab to configure these authentication methods.

DIAT tab

Introduction

Dynamic IP or IPX Address Translation (DIAT) is a unique set of technologies for simplifying deployment of the HomeOffice Router and providing effective and secure network access. A single address represents the entire home or small office network. All of the devices on the HomeOffice Router's LAN share one address.

Note: DIAT is a form of Network Address Translation (NAT).

By default, DIAT for IP and IPX are disabled. You can enable DIAT for IP or IPX networking at any time, for either a single computer or for multiple computers on the HomeOffice Router's LAN.

Sharing an address with multiple hosts

Do not allow more than ten hosts to share an IP or IPX address. If you do so, you experience a degradation in performance due to ISDN bandwidth limitations.

If the Router shares its IP address with multiple hosts, you must also configure the DIAT table. For instructions, see "To configure the DIAT table" on page 248.

DIAT and IP Forwarding

ATTENTION

If you select IP Forwarding in the Ethernet IP Properties, you must select Single Host DIAT in the IP area. IP Forwarding is not compatible with Multi Host DIAT.

To display the DIAT tab

1 Click the ISDN icon.

2 Select Circuits from the pop-up menu that appears.

Result: The Data Circuit Add/Change/Remove screen appears.

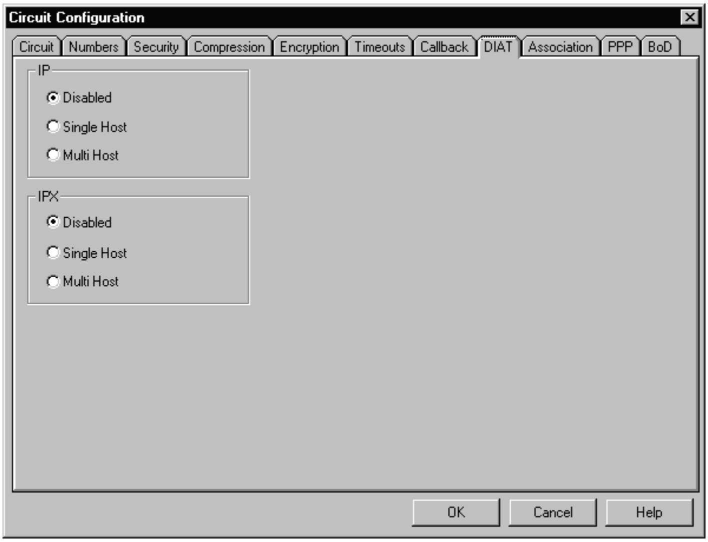
3 Do one of the following:

- Enter a name for the new circuit, and then click Add.
- Select an existing circuit, and then click Change.

Result: The Circuit Configuration screen appears.

4 Click the DIAT tab.

Result: The DIAT tab appears.



IP
● Disabled
○ Single Host
○ Multi Host

IPX
● Disabled
○ Single Host
○ Multi Host

DIAT tab field descriptions

Field	Description
Disabled	Select this option for IP, IPX, or both if the Router's address is not shared with other devices on the LAN.
Single Host	Select this option for IP, IPX, or both if the Router shares its address with only one other host (PC) on the LAN.
Multi Host	Select this option for IP, IPX, or both if the Router shares its address with several hosts (PCs) on the LAN.

Association tab

Introduction

An association links the network protocol address of the remote access switch on the host network to the name of the data circuit on the HomeOffice Router. The Association tab allows you to enter one or both of the following addresses for the destination device:

- an IP address for the IP protocol
- an IPX node address for the IPX protocol

Association

An association binds a protocol to the circuit and allows the circuit name (instead of the network address) to be used when building a route to the destination host network. This feature becomes especially useful if you choose to route over IP using unnumbered links. You must first configure unnumbered links or the destination address in the ISDN properties under the appropriate tab (IP or IPX properties) before the association can be established in the circuit configuration.

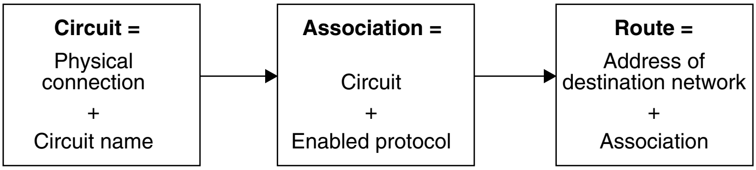
Routes

Once a protocol has been associated with a circuit, you can define a route. You can create a static route (as a default route) to a remote access switch on the host network or to another device accessible by ISDN, such as another telecommuter’s Router. The route for traffic of a certain protocol to a certain destination has then been defined.

Concept diagram

The following diagram shows how a circuit can be associated with a protocol to create a route:

ISG101_D



RIP and SAP

Routing Information Protocol (RIP) is the dynamic routing protocol used on TCP/IP networks. The HomeOffice Router uses RIP over IP, and RIP and Service Advertising Protocol (SAP) over IPX to exchange routing and service information with other routers and to update the information in its Routing table.

You can enable RIP and SAP on both the Ethernet and ISDN interface. You can also enable RIP and SAP on the data circuit.

For more information about RIP and SAP modes, see the following:

- “Routing Information Protocol” on page 223 (for IP networks)
- “Routing Information Protocol” on page 298 (for IPX networks)
- “IPX Services and Service Advertising Protocol” on page 308

RIP version

The HomeOffice Router supports different RIP versions to allow enhanced compatibility with other routers. The following table summarizes the features of each version.

RIP version	Description
Version 1	Does not include subnet information.
Version 2	Includes subnet information.

RIP version	Description
Compatible	Version 2 is backwards-compatible with Version 1.

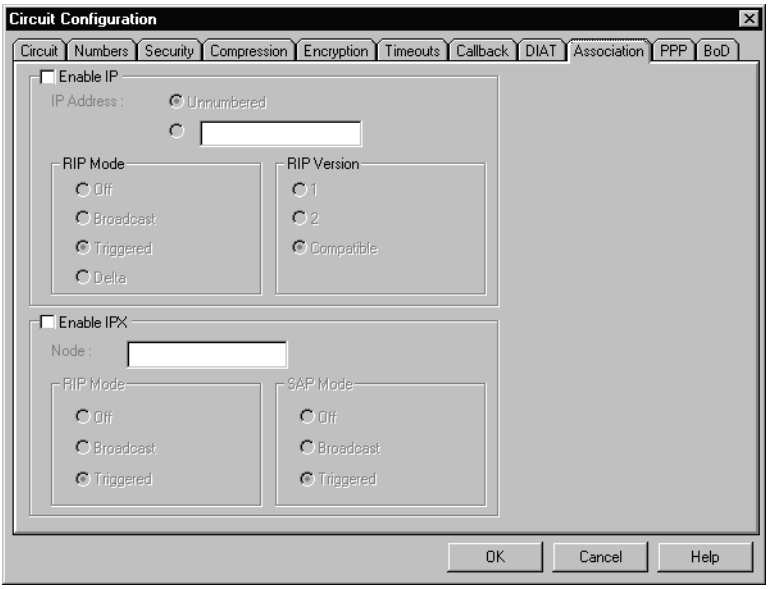
To display the Association tab

1. Click the ISDN icon.
2. Select Circuits from the pop-up menu that appears.

   Result: The Data Circuit Add/Change/Remove screen appears.
3. Do one of the following:
   - Enter a name for the new circuit, and then click Add.
   - Select an existing circuit, and then click Change.

   Result: The Circuit Configuration screen appears.
4. Click the Association tab.

   Result: The Association tab appears.



□ Enable IP

IP Address : ● Unnumbered ○

RIP Mode: ○ Off ○ Broadcast ● Triggered ○ Delta

RIP Version: ○ 1 ○ 2 ● Compatible

□ Enable IPX

Node :

RIP Mode: ○ Off ○ Broadcast ● Triggered

SAP Mode: ○ Off ○ Broadcast ● Triggered

Association tab field descriptions

Field	Description
Enable IP	Select this option if you want to enable IP routing on this circuit.
IP Address	If you do not want to use unnumbered links, select this option and then enter the IP address of the destination to which you want to connect with this circuit. You can enter an IP address on this circuit only if you also enter an IP address in the ISDN Properties.
Unnumbered	Select this option if you want to use unnumbered links. You can select this option on the circuit only if you also select Unnumbered in the ISDN Properties.
IP RIP Mode	Select the RIP mode to be used on this circuit. • Off: If you select this option, you must set up static routes. To create static routes, use the IP Properties option from the Admin icon pop-up menu. • Broadcast: If you select this option, RIP messages are sent every 30 seconds. If the link is not up, the link is opened for these messages. • Triggered: If you select this option, RIP messages are sent only when the Routing table changes. If the link is not up, the link is opened for these messages. • Delta: If you select this option, RIP messages are sent only when the link is already up for other reasons. If the link is not up, these messages are not sent. This reduces traffic and connection costs.

Field	Description
IP RIP Mode (continued)	If you are connecting to an Intel Shiva LanRover Access Switch, select Delta for the most efficient, cost-effective connection. In general, use Triggered over an ISDN connection, because this setting affects only this circuit, not the entire interface. **Note:** If the ISDN address to call is set to DISABLED on this circuit, you must disable Triggered RIP as outgoing calls cannot be made on this circuit.
IP RIP Version	Select the RIP version you want to use: • V1: Select this option if the Router connects to a small network without subnets, or to a network that is also using RIP V1. • V2: Select this option if the Router connects to a large network that is subnetted, or if you know that the remote network is also using RIP V2. If you select RIP V2, you do not need to set up static routes from the remote access switch to the HomeOffice Router. (**Note:** The remote access switch on the remote network must also be running RIP V2.) • Compatible: Select this option if you are not sure which version is being used on the network. **Note:** RIP V1 and V2 can run in Triggered or Broadcast mode.
Enable IPX	Select this option if you want to enable IPX routing on this circuit.

Field	Description
Node	Enter the Node address of the destination to which you want to connect with this circuit. The node address must be 12 hexadecimal digits. **Note:** You do not need to enter the network address as the Router can work this out.
IPX RIP Mode	Select the RIP mode to be used on this circuit: • Off: If you select this option, you must set up static routes. To create static routes, use the IPX Route dialog. • Broadcast: If you select this option, RIP messages are sent every 30 seconds. • Triggered: If you select this option, RIP messages are sent when the Routing table changes. In general, use Triggered for ISDN as this setting only affects this circuit, not the entire interface.
IPX SAP Mode	Select the SAP mode to be used on this circuit: • Off: If you select this option, you must set up static routes. To create static routes, use the IPX Route dialog. • Broadcast: If you select this option, SAP messages are sent every 30 seconds. • Triggered: If you select this option, SAP messages are sent when the Routing table changes. In general, use Triggered for ISDN as this setting only affects this circuit, not the entire interface. **Note:** If the ISDN address to call is set to DISABLED on this circuit, you must disable Triggered SAP as outgoing calls cannot be made on this circuit.

PPP tab

Introduction

Use the PPP tab to configure PPP timers. PPP timers make checks on the time taken to negotiate links between devices.

Note: In normal circumstances, you do not need to change the PPP timer values, as they are the default values for any router using the standard PPP setup. It is important that they are identical in both the original and target routers.

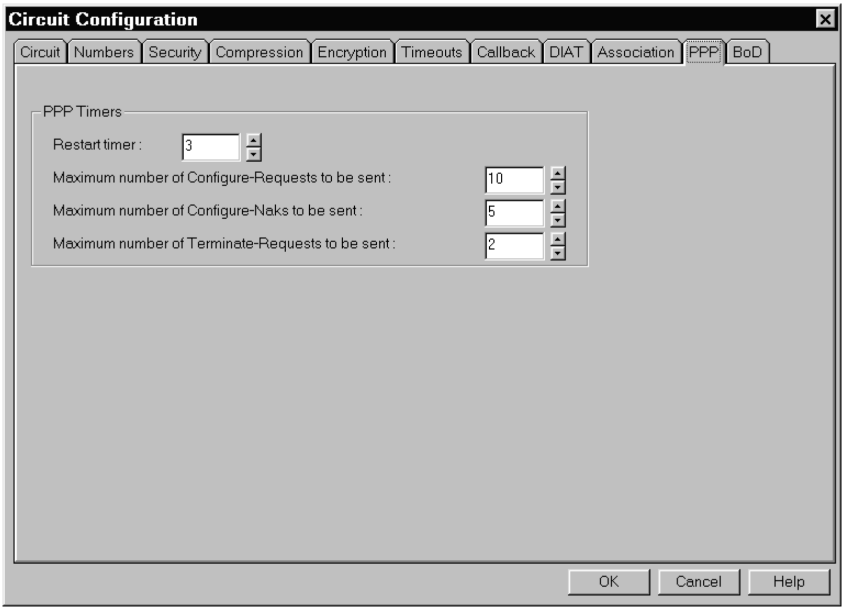
To display the PPP tab

1. Click the ISDN icon.
2. Select Circuits from the pop-up menu that appears.

   Result: The Data Circuit Add/Change/Remove screen appears.
3. Do one of the following:
   - Enter a name for the new circuit, and then click Add.
   - Select an existing circuit, and then click Change.

   Result: The Circuit Configuration screen appears.
4. Click the PPP tab.

   Result: The PPP tab appears.



PPP Timers

Restart timer : 3

Maximum number of Configure-Requests to be sent : 10

Maximum number of Configure-Naks to be sent : 5

Maximum number of Terminate-Requests to be sent : 2

PPP tab field descriptions

Field	Description
Restart timer	Enter a value between 1 and 16 seconds. The default is 3.
Maximum number of Configure-Requests to be sent	Enter a value between 1 and 10 seconds. The default is 10.
Maximum number of Configure-Naks to be sent	Enter a value between 1 and 10 seconds. The default is 5.
Maximum number of Terminate-Requests to be sent	Enter 1 or 2. The default is 2.

BoD tab

Introduction

The HomeOffice Router allows the ISDN interface to temporarily provide additional bandwidth by using more virtual circuits when available. This is known as Bandwidth On Demand.

The Bandwidth on Demand (BoD) tab allows you to do the following:

- Set up two or more ISDN B-channels to provide more bandwidth.
  This is known as Aggregation and is done using PPP Multilink.
- Set thresholds for increasing bandwidth.
  These thresholds determine when additional virtual circuits are opened.

Prerequisites

Before you can configure Bandwidth on Demand, you must select two B-channels on the Circuit tab. By selecting two B-channels, you can use more than one virtual circuit to reach a destination.

Benefits of bandwidth aggregation

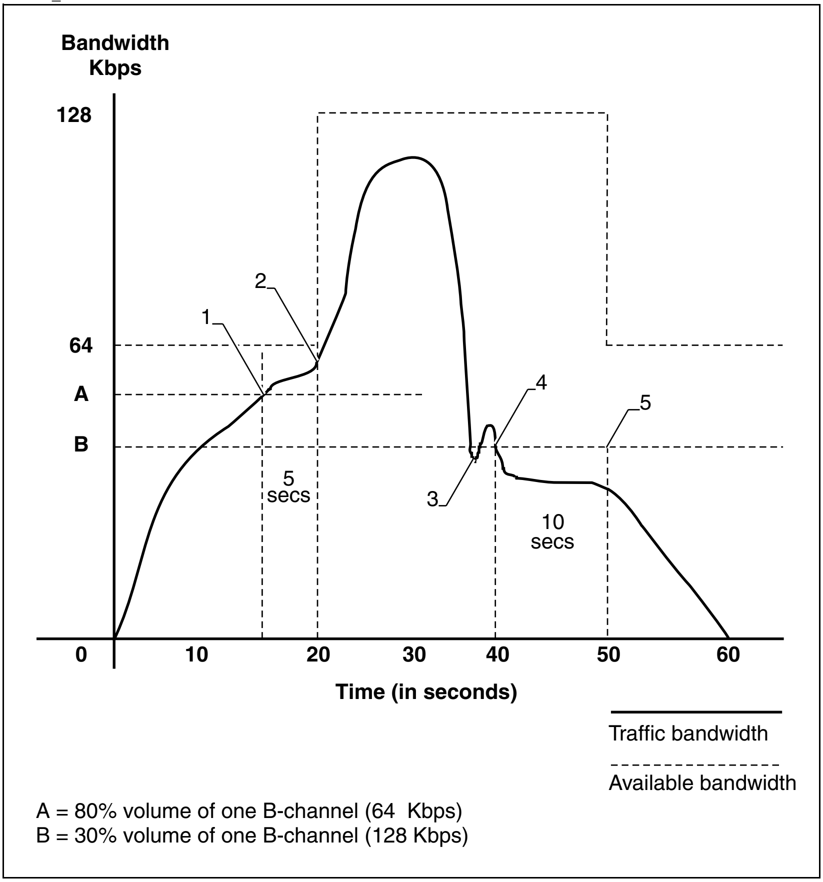
Bandwidth aggregation occurs dynamically on an as-needed basis. Before you begin to set up aggregation, you must decide at what point you want the second B-channel to open. For example, you may want to open the second channel when the first is at 80% of its maximum throughput. You must also work out how long you want traffic on the first B-channel to remain at this percentage level before the second channel opens up.

How aggregation works

The following description and illustration explain how aggregation works:

1. When an ISDN call is made, one B-channel is opened.
2. In the illustration that follows, Point 1 shows when data reaches the traffic load percentage value. This means that the volume of data has reached the configured percentage value. You can configure the HomeOffice Router to wait for a set length of time before bringing the second B-channel into operation, or you can configure it to open when a sudden burst causes this value to be exceeded. In this case, data volume must exceed 80% volume for a certain length of time (5 seconds) before the second B-channel is opened.
3. Point 2 marks the point at which data volume has exceeded the traffic load percentage value for 5 seconds. The second ISDN B-channel now opens automatically, and remains open until data volume drops below a configurable level. Data is shared equally between the two B-channels.
4. At point 3 in the illustration, traffic decreases temporarily before increasing again. Because bandwidth requirements can change suddenly like this, the second B-channel waits for a period of time before closing down. In the following illustration, this value has been set to 10 seconds. You can set this time to suit your own requirements.
5. At point 4, data drops below the lower traffic load percentage value. Because traffic volume must remain below this threshold for a certain length of time, the second B-channel does not close until point 5 has been reached (10 seconds later).
6. The ISDN link closes when traffic stops.

ISG102_D



A = 80% volume of one B-channel (64 Kbps)
B = 30% volume of one B-channel (128 Kbps)

Bandwidth Allocation Control Protocol

The Bandwidth Allocation Control Protocol (BACP) allows you to coordinate the addition and removal of B-channels from a bundle interface. This prevents one end from opening another B-channel to accommodate extra data, and the other end from closing it down immediately. When one device wants to increase bandwidth, it contacts the other device and requests that a new B-channel be opened. Both ends must agree to open or close a B-channel before any action is taken.

Enable BACP by using the `network general multilink` command in the command shell. To fine-tune BACP parameters, use the `network isdn2 bap` command.

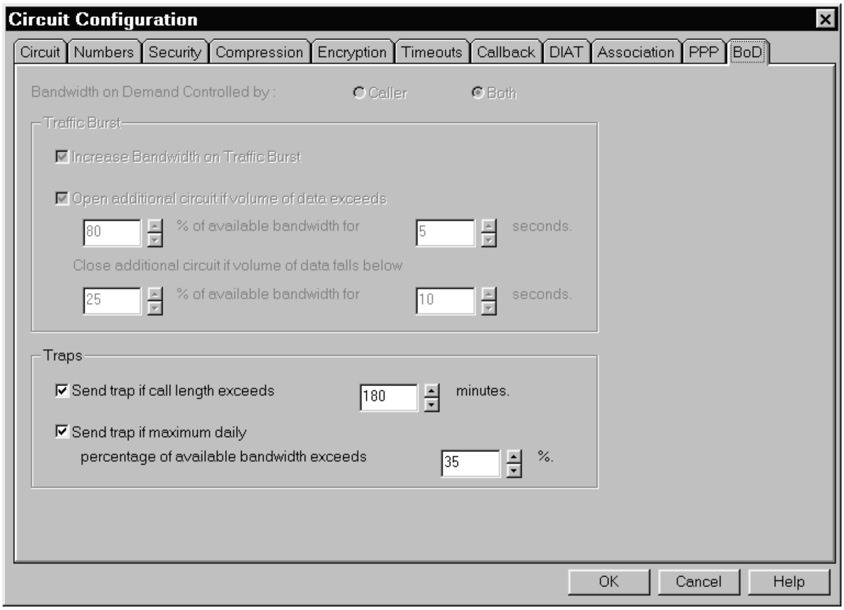
To display the BoD tab

1. Click the ISDN icon.
2. Select Circuits from the pop-up menu that appears.

   Result: The Data Circuit Add/Change/Remove screen appears.
3. Do one of the following:
   - Enter a name for the new circuit, and then click Add.
   - Select an existing circuit, and then click Change.

   Result: The Circuit Configuration screen appears.
4. Click the BoD tab.

   Result: The BoD tab appears.



Bandwidth on Demand Controlled by : ○ Caller ● Both

Traffic Burst

☑ Increase Bandwidth on Traffic Burst

☑ Open additional circuit if volume of data exceeds

80 % of available bandwidth for 5 seconds.

Close additional circuit if volume of data falls below

25 % of available bandwidth for 10 seconds.

Traps

☑ Send trap if call length exceeds 180 minutes.

☑ Send trap if maximum daily percentage of available bandwidth exceeds 35 %.

BoD tab field descriptions

Field	Description
Bandwidth on Demand Controlled by	Select one of the following options for initiating Bandwidth on Demand: • Caller: If the Router is interoperating with another Nortel Networks device, vendor's device, or HomeOffice Router. If you are using two HomeOffice Router, both ends of the link should use the same setting. • Both: If the Router is interoperating with a Router that is running pre-V6 software, or you want both ends of the link to be able to initiate additional calls to aggregate or augment the initial call.
Increase Bandwidth on Traffic Burst	If you select this option, a new virtual circuit opens and traffic transfers onto it when a sudden burst of data occurs. If you leave this check box blank, data transmission remains only on the existing virtual circuit during a sudden burst.
Open additional circuit if volume of data exceeds	If you select this option, an additional virtual circuit opens and data transfers onto it when the volume of data on the existing virtual circuit exceeds the specified threshold value for a set length of time (see step 2 on page 191). Do the following: **1** Select this option to open an additional circuit. **2** Enter the percentage level that the volume of data on the existing virtual circuit must reach before an additional virtual circuit is brought into use. The default is 80%.

Field	Description
Open additional circuit if volume of data exceeds (continued)	**3** Enter the length of time for which data must reach (or exceed) the volume that you have set before an additional virtual circuit opens for data. The second virtual circuit is used for aggregation and data is shared between the two virtual circuits. The default is 5 seconds. If you do not select this option, data transmission remains on the existing virtual circuit.
Close additional circuit if volume of data falls below	**1** Select this option to close the additional circuit. **2** Enter the percentage level that the volume of data on the second virtual circuit must fall to before this circuit is closed. The range is 0 to 40 seconds. When data transmission on the second virtual circuit falls below the specified level for a sustained length of time (see step 4 on page 191), traffic transfers back to the original virtual circuit. **3** Enter the length of time for which data must fall below the specified volume. You can set a time between 5 and 60 seconds. For example, if you keep the default values, the second virtual circuit automatically closes down when its data levels fall below the threshold of 25% for 10 seconds.
Send trap if call length exceeds	Enter the maximum length of an ISDN call between 1 and 9999 minutes. The default is 180 minutes. If this limit is exceeded, a trap is sent.

Field	Description
Send trap if maximum daily percentage of available bandwidth exceeds	Enter the maximum daily percentage of available bandwidth to be used for calls (ISDN). The value that you set should take into account the number of virtual circuits available. For example, if two virtual circuits are open, they trigger a trap when they have been open for half of the percentage specified here. If this percentage is exceeded, an SNMP trap is sent. The default is 35.

Section D: Configuring the IP network

In this section

Overview

Introduction

This section describes TCP/IP features, when and why they should be used, and how to configure them.

IP address and subnet mask

Use IP addresses to uniquely identify each host on the network. On the HomeOffice Router, IP addresses are assigned to each interface (Ethernet and ISDN) to facilitate routing and forwarding between network devices.

Alternatively, you can set ISDN IP addresses on your Router to be *unnumbered*. By doing this, you can route IP over a link between two devices without assigning an IP address to the ISDN interfaces. This allows you to save valuable IP address space.

If required, you can use subnet masks to subdivide a network into smaller networks. Subnet masks provide you with much more flexibility when allocating IP addresses, and ensure that network traffic is not sent to the whole network unintentionally.

IP Routing

Routing is the process of selecting the correct interface and next hop for a packet being forwarded to another network device. Routes identify the destination IP address, next hop, and the number of hops used to reach the destination.

A hop is one data link in the path to the final destination. On the HomeOffice Router, you can define the next hop as one of the following:

- an IP address
- circuit name

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is a TCP/IP protocol that manages the distribution of TCP/IP-related configuration information by DHCP servers. The servers allocate IP addresses automatically to clients configured to use DHCP. When a DHCP client boots to the network, it can request IP-related information such as the following from the server:

- an IP address
- subnet mask
- default gateway
- DNS and WINS server addresses

You can configure the HomeOffice Router as a DHCP server for the telecommuter's LAN.

Routing Information Protocol

Routing Information Protocol (RIP) is the dynamic routing protocol used on TCP/IP networks. The HomeOffice Router uses RIP over IP to exchange routing information with other routers and to update the information in its routing table.

RIP is available on both the Ethernet and ISDN interfaces. You may decide not to run RIP on the ISDN interface to reduce costs. However, you should keep RIP running on the Ethernet (LAN) interface, because this does not affect connection costs.

DIAT for IP

Dynamic IP Address Translation (DIAT for IP) is a mechanism by which a remote network of one or more devices can appear as a single dial-in user to the host network. This allows the remote network the flexibility to implement an addressing scheme that is invisible to the host network.

DIAT for IP is a form of Network Address Translation (NAT) used on other vendors' routers.

IP Forwarding

When DIAT for IP is enabled, you can use a single PC with any IP address to gain network connectivity. You can use IP Forwarding with DIAT for IP so that the HomeOffice Router can forward the PC's requests. With DIAT for IP and IP Forwarding enabled, a telecommuter can have the same configuration both at home and in the office.

Broadcast Forwarding and IP Relay

A broadcast is a network transaction that sends data to one or more hosts connected to the network. The addresses to which the broadcast is being sent may be the broadcast addresses of a remote IP network or the IP address of a server itself.

Forwarding is the process by which the Router sends requests from a server on its network to another server on the same or other network. Forwarding is completed according to entries in the Router's IP Relay table.

Note: Windows NT and BootP environments often need Broadcast Forwarding.

Spoofing

Spoofing is the process by which the HomeOffice Router prevents meaningless traffic from keeping the network connection open. The Ethernet interface settings control some kinds of IP spoofing that the HomeOffice Router performs. This lets you determine, for some kinds of network traffic, whether the packets are meaningful.

Bridging

Bridging offers one of the most straightforward and flexible methods of interconnecting network segments. Bridges are very simple to use. No changes are required to existing applications or communications software when you introduce bridges to a network.

If you set up the HomeOffice Router as a bridge/router, then IP is routed across the interfaces that have the IP protocol enabled, while all other protocols (DECnet, AppleTalk, Banyan Vines, SNA, and so on) are bridged.

IP address and subnet mask

Introduction

This section explains what an IP address and subnet mask are, and explains how to configure them for the Ethernet and ISDN interfaces.

IP address

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

The IP address assigned to each HomeOffice Router interface (Ethernet and ISDN) must be unique, and should conform to the addressing scheme used on your network. The ISDN and Ethernet interfaces must be on different networks.

Using IP Forwarding

If you are configuring for IP Forwarding, the Ethernet IP address of the HomeOffice Router must be on a different IP network to the telecommuter's PC.

Note: Local Manager allows you to configure only one IP address per interface and one for bridging.

Using IP Routing

If you are configuring for routing, the Ethernet interface and the ISDN interface must be on different networks.

Subnet masks

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

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

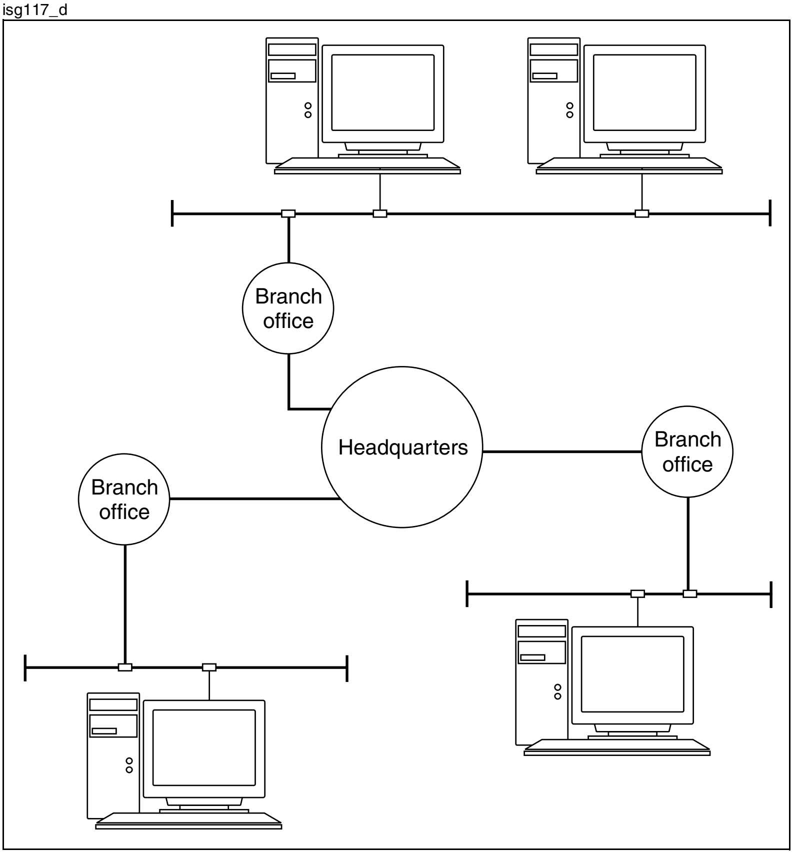
What is a subnet mask?

The 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 HomeOffice Router what portion of the IP address represents the network (and sub-network) and what portion represents the host.

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

Example of subnet use

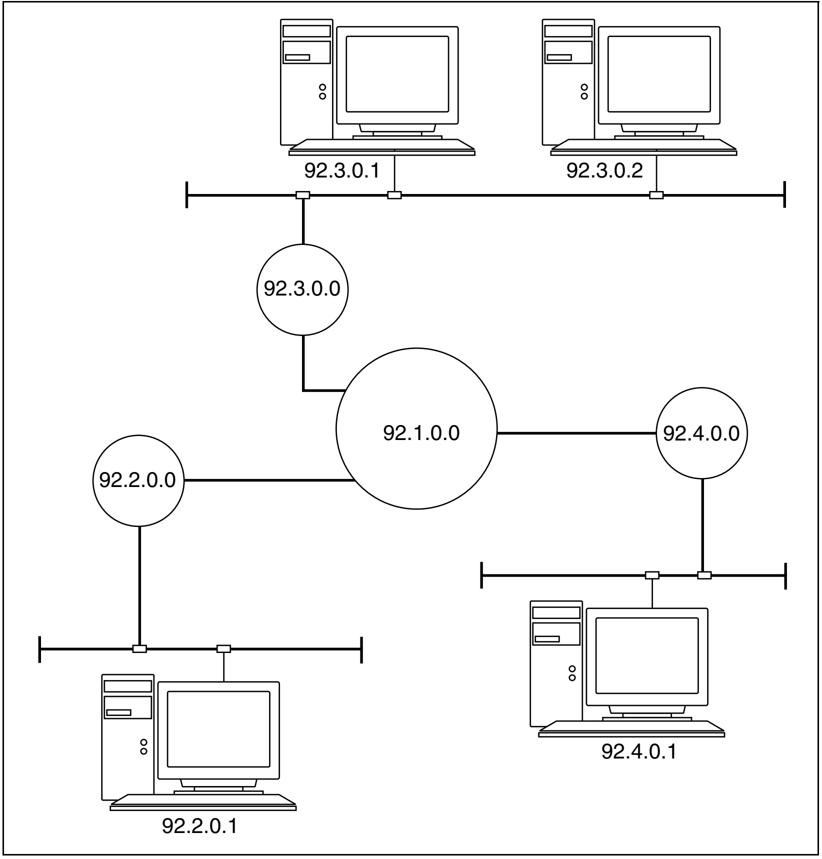
The following illustration shows a typical setup for an organization with headquarters and branch offices.



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

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

isg118_d



In this case, the subnet mask is 255.255.0.0. This tells the HomeOffice Router that the first 16 bits of the IP address represent the network and subnetwork.

Note: In this example, the PCs and HomeOffice Routers are set up to have the same subnet mask.

Numbered and unnumbered links

You can set up LAN and WAN interfaces on the HomeOffice Router to be numbered or unnumbered.

Numbered links

When using numbered links, the ISDN network acts as a unique IP network over which your HomeOffice Router connects to a remote router. You must assign an IP address to your HomeOffice Router's ISDN interface to identify your HomeOffice Router as a node on this network.

Note: You can use numbered links only if you are connecting to another router that supports numbered links.

Unnumbered links

Unnumbered links mean that you do not have to assign IP addresses to the interfaces, allowing you to save valuable IP address space. For instructions on creating an unnumbered link, see "Unnumbered links" on page 235.

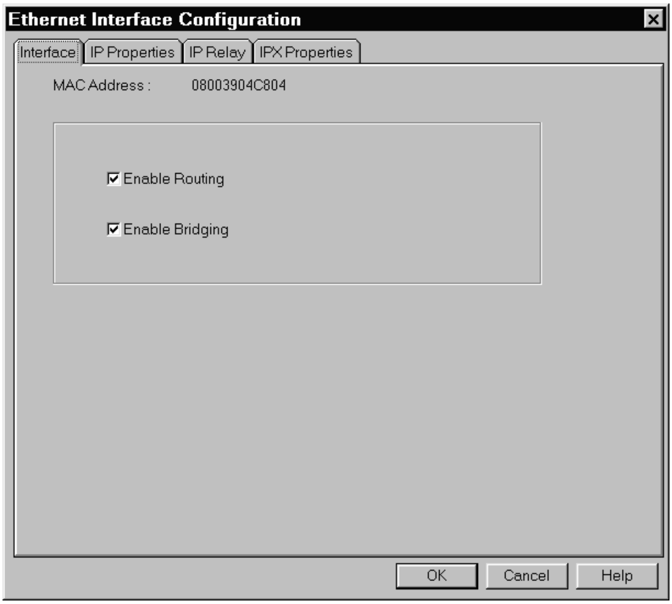
When to use a numbered link

The numbered link option allows the HomeOffice Router to be another recognized routing device extending off the main host network. The HomeOffice Router can provide connectivity to another subnetted LAN within the telecommuter's Ethernet network. Under this circumstance, you can configure the Router with static (or dynamic) addresses to route data between the LANs and pass routing information (RIP) in a similar manner to a conventional network router.

To configure the IP address and subnet mask on the Ethernet interface

1. Click the Ethernet icon.
2. Select Properties from the pop-up menu that appears.

   Result: The Ethernet Interface Configuration screen appears.



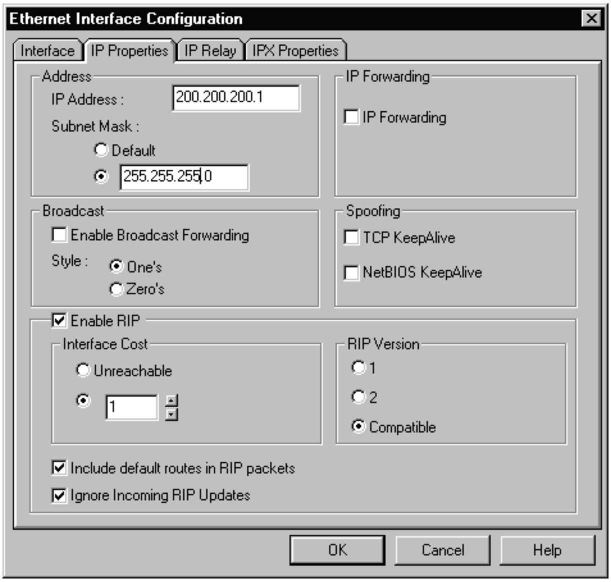
MAC Address : 08003904C804

☑ Enable Routing

☑ Enable Bridging

3 Click the IP Properties tab.

Result: The IP Properties tab appears.



Address

IP Address : 200.200.200.1

Subnet Mask :

○ Default

● 255.255.255.0

IP Forwarding

☐ IP Forwarding

Broadcast

☐ Enable Broadcast Forwarding

Style : ● One's ○ Zero's

Spoofing

☐ TCP KeepAlive

☐ NetBIOS KeepAlive

☑ Enable RIP

Interface Cost

○ Unreachable

● 1

RIP Version

○ 1

○ 2

● Compatible

☑ Include default routes in RIP packets

☑ Ignore Incoming RIP Updates

4 Enter the IP address for the Ethernet interface.

5 For the Subnet Mask, do one of the following:

- Click Default to define 255.0.0.0 as the subnet mask.
- Enter a specific subnet mask.

6 Click OK.

Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

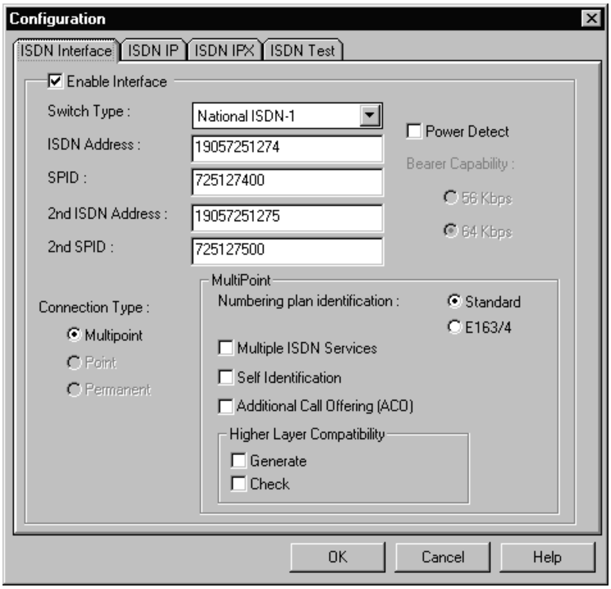
To configure the IP address and subnet mask on the ISDN interface

Note: Before you can enter the IP address for the ISDN interface, you must ensure that the ISDN interface is configured with valid ISDN directory numbers and SPIDs. For instructions, see “Configuring the ISDN interface” on page 107.

1 Click the ISDN icon.

2 Select Properties from the pop-up menu that appears.

Result: The Configuration screen appears.



Configuration

☑ Enable Interface

Switch Type : National ISDN-1

ISDN Address : 19057251274

SPID : 725127400

2nd ISDN Address : 19057251275

2nd SPID : 725127500

□ Power Detect

Bearer Capability : ○ 56 Kbps ● 64 Kbps

Connection Type : ● Multipoint ○ Point ○ Permanent

MultiPoint

Numbering plan identification : ● Standard ○ E163/4

□ Multiple ISDN Services

□ Self Identification

□ Additional Call Offering (ACO)

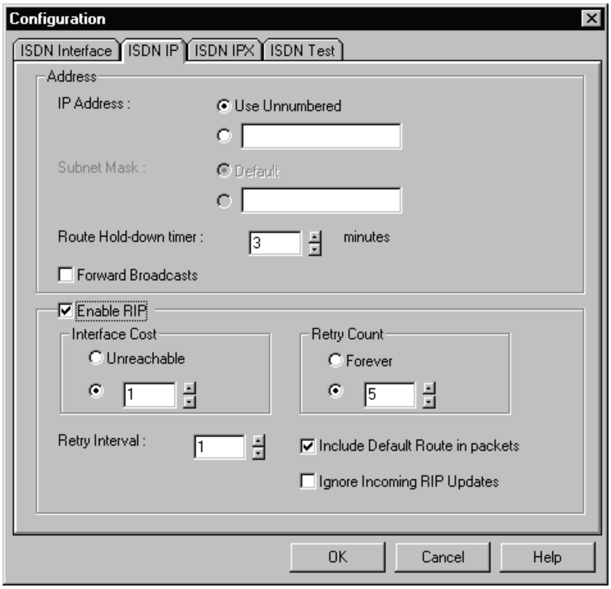
Higher Layer Compatibility

□ Generate

□ Check

3 Click the ISDN IP tab.

Result: The ISDN IP tab appears.



Address

IP Address : ● Use Unnumbered ○

Subnet Mask : ● Default ○

Route Hold-down timer : 3 minutes

□ Forward Broadcasts

☑ Enable RIP

Interface Cost: ○ Unreachable ● 1

Retry Count: ○ Forever ● 5

Retry Interval : 1

☑ Include Default Route in packets

□ Ignore Incoming RIP Updates

4 Click the button next to the IP address box, and then enter the IP address for the ISDN interface.

5 For the Subnet Mask, do one of the following:

- Click Default to define 255.255.255.255 as the subnet mask.
- Click the button next to the subnet mask box, and then enter a specific subnet mask.

6 Click OK.

Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

IP Routing

Introduction

Routing is the process of selecting the correct interface and next hop for a packet being forwarded to another network device. Routes identify the destination IP address, next hop, and the number of hops used to reach the destination.

A hop is one data link in the path to the final destination. You can define the next hop as one of the following:

- an IP address
- a circuit name

Configuration overview

Note: Review this section completely before beginning any configuration.

To configure Routing for the Ethernet interface

1. Enable Routing on the Ethernet interface (see page 213).
2. Enter static routes into the IP Routes table (see page 217).

To configure Routing for the ISDN interface

1. Enable Routing on an ISDN circuit (see page 214).
2. Define the route hold-down timer on the ISDN interface (see page 215).
3. Enter static routes into the IP Routes table (see page 217).

When to use Routing

Routing should be the first option configured to maximize Router features such as DIAT for IP and demand mode circuits. Routing minimizes the period in which the ISDN line is active.

Types of routing

Static routing

Routes that are defined in a routing table are static routes. To select a suitable route, the Router first identifies the network to which the packets are being sent, and then selects a route with a matching destination network address.

If you choose static routing for the dialup connection, a route is generally defined to the host network. In most telecommuter dialup configurations, a default route to the next hop remote access switch is sufficient. This default route is defined on the HomeOffice Router when the Install Wizard is used to configure a circuit. If additional routes are required (to other telecommuter units for example), you must consider routing table capacity and administrative requirements.

Dynamic routing

If your host computers understand Routing Information Protocol (RIP), you can use RIP on both the ISDN and Ethernet interfaces of the HomeOffice Router. RIP automatically updates each host's routing table.

If you want to use dynamic routing, see "Routing Information Protocol" on page 223 for more information.

Benefits and drawbacks of using Routing

Benefits

Routing

- provides an efficient method of managing network traffic
- reduces the effect of network broadcast packets
- enables network interface devices to maintain updated routing information

Drawbacks

Routing

- requires additional consideration in network planning details

- does not inherently pass all of the types of protocols without additional provisioning
- requires additional administration

When to use the routing table

If a telecommuter connects only to a central site on the corporate network, the only route that is required is a default route to the remote access switch interface. When configuring the telecommuter’s circuit with the Install Wizard, a default circuit is created and subsequently is the only route configured in the IP Routing table. A routing table is required, even if it contains only one route (the default route).

You can configure up to 32 static entries in the IP Routing table. Statically entered routing addresses (stored permanently in the IP Routing table) define the routes by which the HomeOffice Router reaches remote networks. You can enter up to three static routes to any remote network.

Prerequisites for static routes over ISDN

Before adding ISDN routes to the IP routing table, ensure that you do the following:

- Set up the ISDN interface using the ISDN Interface dialog.

  For instructions, see “Configuring the ISDN interface” on page 107.
- Decide on the addressing information that you require.

  In this case, you require the IP addresses of the remote devices and the ISDN addresses of the ISDN interfaces. You should also think of an appropriate name for the circuit.

How multiple static routes work

Multiple static routes are a cost-saving alternative to running RIP over WAN links.

The HomeOffice Router detects if the best route (as defined by the metric value) becomes unavailable, and uses the next best route. If the original best route returns to service, it replaces the alternative route. Since the Router determines which route to use, you do not need to run RIP over the ISDN link.

When a static route is detected as being down (that is, when the physical link breaks), it can take up to three minutes for an alternative route to be used. This is the length of time that it takes for RIP running on either side of the ISDN link to broadcast the routing topology change throughout the network. RIP normally works in this way.

You may decide that static routes provide the network resilience you require, while avoiding the possible expense of standard RIP, or the limitations of Triggered RIP.

Connecting networks

LANs connected by routers must have different network addresses. If your networks were previously connected by a bridge, or if your LAN was not previously connected to other LANs (through a WAN), you must ensure that the network address of each LAN is distinct. This can mean that you must change the IP addresses of all hosts on one of the LANs to a new network address.

Add an entry for the WAN network to the host's routing table if you want to allow calls from remote HomeOffice Routers to be made into your host. Although calls to a HomeOffice Router can be made into either of its IP addresses, calls from a remote HomeOffice Router use the WAN address. The HomeOffice Router always uses the correct IP address for outgoing calls to the appropriate network.

Route hold-down timer

The route hold-down timer applies only to the ISDN interface.

When the Router realizes that an ISDN circuit is not responding, it deletes all routes dependent on that circuit. The route hold-down timer is the number of minutes that should elapse between your Router realizing that a circuit has gone down and the deletion of all dependent routes.

A route hold-down timer of 3 minutes is recommended. A value of less than 3 minutes may be appropriate when a faster response to the failure of a circuit is required. This is recommended only if the device is operating on a leaf node of the network. Within a mesh, changing this timer may have unpredictable results if other RIP entities are running with the default timing.

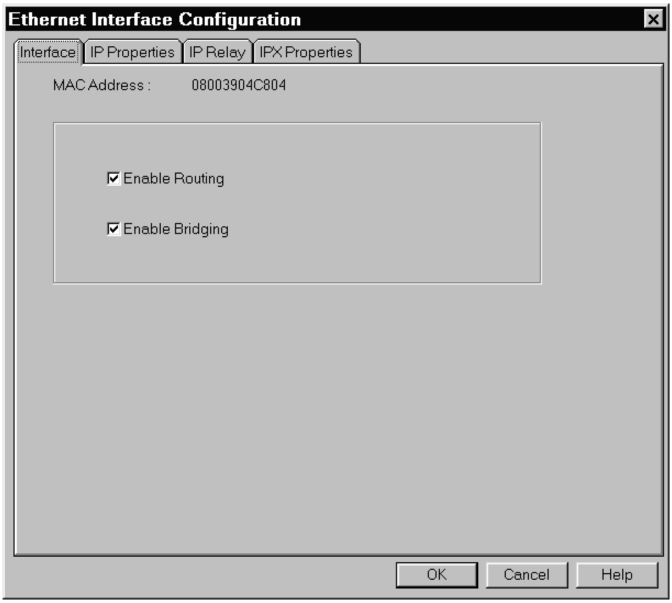
The default of 3 minutes is suitable for most situations. If you increase this timer, then it has the effect of reducing the number of network reconfigurations on networks that suffer short-term link failures or congestion. The network also takes longer to reconfigure when a permanent link failure occurs.

To enable Routing on the Ethernet interface

1 Click the Ethernet icon.

2 Select Properties from the pop-up menu that appears.

Result: The Ethernet Interface Configuration screen appears.



Ethernet Interface Configuration

MAC Address : 08003904C804

☑ Enable Routing

☑ Enable Bridging

3 Ensure that Enable Routing is selected.

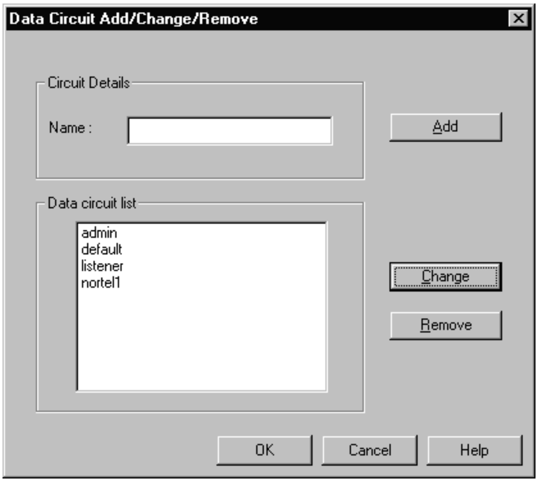
4 Click OK.

Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

To enable Routing on the ISDN circuit

1. Click the ISDN icon.
2. Select Circuits from the pop-up menu that appears.

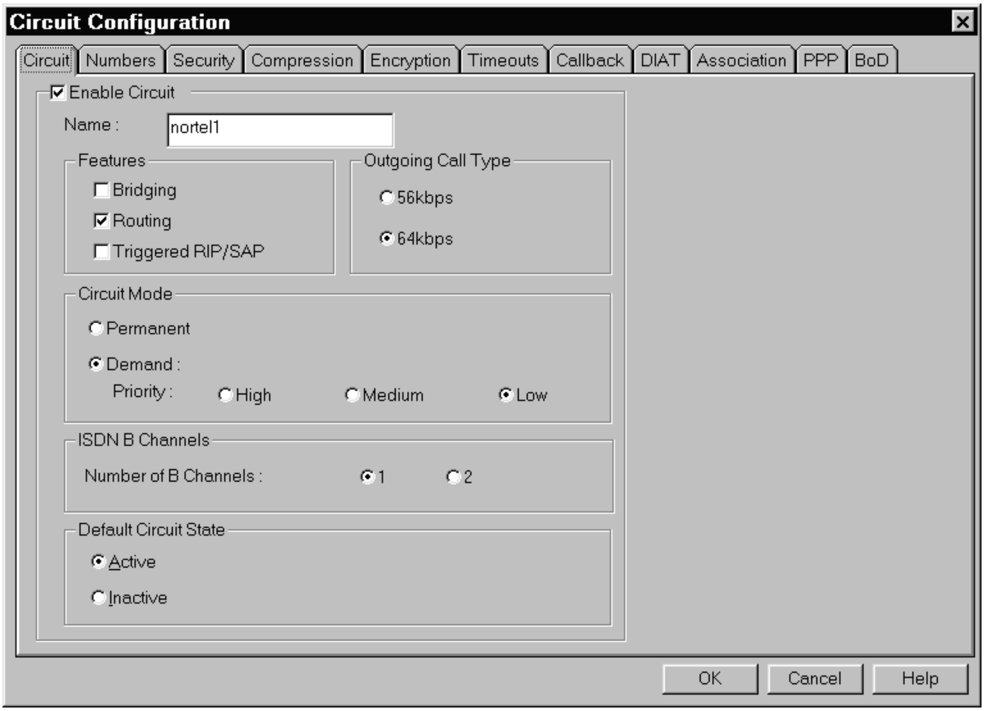
   Result: The Data Circuit Add/Change/Remove screen appears.



admin
default
listener
nortel1

3. Select the circuit for which you want to enable Routing, and then click Change.

   Result: The Circuit Configuration screen appears.



☑ Enable Circuit

Name : nortel1

Features
☐ Bridging
☑ Routing
☐ Triggered RIP/SAP

Outgoing Call Type
○ 56kbps
● 64kbps

Circuit Mode
○ Permanent
● Demand :
Priority : ○ High ○ Medium ● Low

ISDN B Channels
Number of B Channels : ● 1 ○ 2

Default Circuit State
● Active
○ Inactive

4 On the Circuit tab, ensure that Routing is selected.

5 Click OK.

Result: The Data Circuit Add/Change/Remove screen appears.

6 Click OK again.

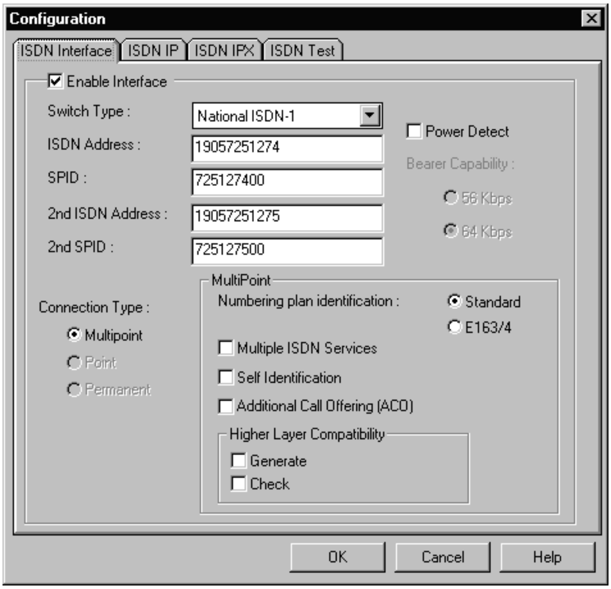
Result: You return to the Configuration tab.

To configure the route hold-down timer on the ISDN interface

1 Click the ISDN icon.

2 Select Properties from the pop-up menu that appears.

Result: The Configuration screen appears.



Configuration

ISDN Interface | ISDN IP | ISDN IPX | ISDN Test

☑ Enable Interface

Switch Type : National ISDN-1

ISDN Address : 19057251274

SPID : 725127400

2nd ISDN Address : 19057251275

2nd SPID : 725127500

□ Power Detect

Bearer Capability :

○ 56 Kbps

● 64 Kbps

Connection Type :

● Multipoint

○ Point

○ Permanent

MultiPoint

Numbering plan identification : ● Standard ○ E163/4

□ Multiple ISDN Services

□ Self Identification

□ Additional Call Offering (ACO)

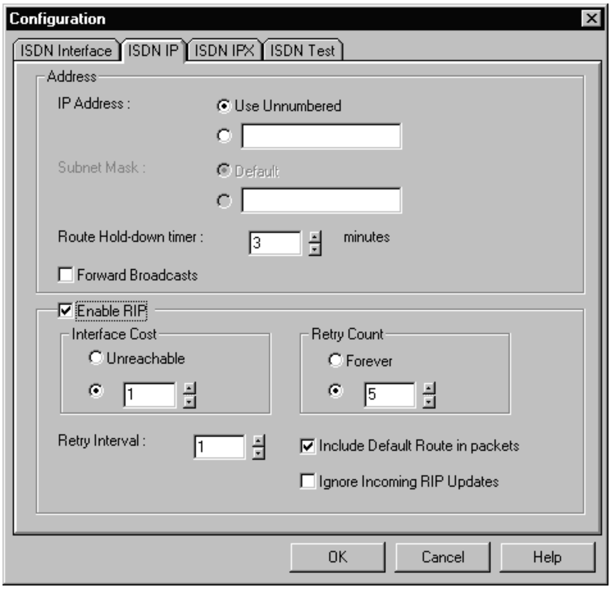
Higher Layer Compatibility

□ Generate

□ Check

3 Click the ISDN IP tab.

Result: The ISDN IP tab appears.



Configuration

ISDN Interface | ISDN IP | ISDN IPX | ISDN Test

Address

IP Address : ● Use Unnumbered

○

Subnet Mask : ● Default

○

Route Hold-down timer : 3 minutes

□ Forward Broadcasts

☑ Enable RIP

Interface Cost

○ Unreachable

● 1

Retry Count

○ Forever

● 5

Retry Interval : 1

☑ Include Default Route in packets

□ Ignore Incoming RIP Updates

4 In the Route Hold-down timer box, enter the number of minutes (between 0 and 1440), that you want to elapse between your Router realizing that a circuit has gone down and the deletion of all dependent routes.

5 Click OK.

Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

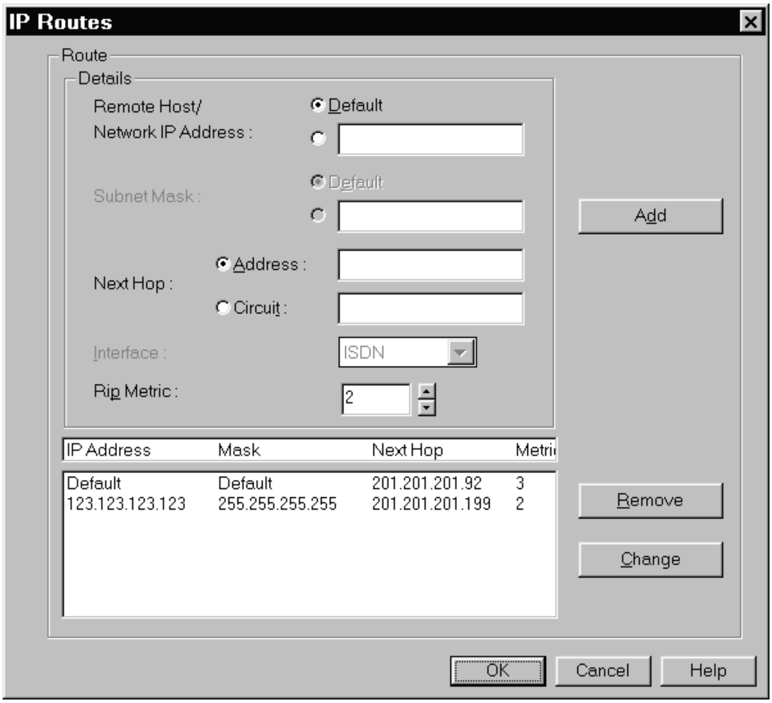
To create IP routes

Note: If two routes have identical names, the Router uses the static route and ignores the dynamic route.

1 Click the Admin icon.

2 Select IP Properties from the pop-up menu that appears.

Result: The IP Routes screen appears.



IP Routes

Route

Details

Remote Host/ Network IP Address : ● Default ○

Subnet Mask : ● Default ○

Next Hop : ● Address : ○ Circuit :

Interface : ISDN

Rip Metric : 2

IP Address	Mask	Next Hop	Metri
Default	Default	201.201.201.92	3
123.123.123.123	255.255.255.255	201.201.201.199	2

3 Complete the fields as described in “Routing table field descriptions” (below).

4 Click Add.

Result: If all of the entries are valid, the route is added to the table at the bottom of the screen. If one or more entries are not valid, an error message appears.

5 Click OK.

Result: You return to the Configuration tab.

Routing table field descriptions

Field	Description
Remote Host/ Network IP Address	Click Default or enter the name or address of the final destination network. The IP address must be in decimal format and must not be a network to which the Router is directly connected. **Note:** You can add up to three routes to the same destination network.
Subnet Mask	If you chose to enter an IP address for the remote device, then this field is enabled. If the network is complex with many subnets, then enter the subnet mask for the route. Otherwise, click Default.
Next Hop	Click Address if you want to enter the IP address of the next router in line towards the destination network. The next hop node must be on a network to which the Router is connected. Click Circuit if you want to enter the circuit name and ISDN interface of the next hop router. **Note:** If the circuit is associated with an IP address, then the IP address appears in the Next Hop column when the route is added to the table.

Field	Description
Interface	The Interface list box is enabled when you choose to create a route using a circuit. Ensure that the ISDN interface is selected. **Note:** This release does not support the X25D interface listed in the Interface list box.
RIP Metric	Enter the number of hops (or routers) that it takes to reach the destination network. The number of hops is the number of routers that traffic must travel through to reach the destination. This must be between 1 and 15. Packets are sent over the route with the lowest metric. **Note:** You can enter an artificially high or low metric to force the Router to use (or not use) a particular route. The default is 2.

Dynamic Host Configuration Protocol

Introduction

Dynamic Host Configuration Protocol (DHCP) is a TCP/IP protocol that manages the distribution of TCP/IP-related configuration information by DHCP servers. The servers allocate IP addresses automatically to clients configured to use DHCP. When a DHCP client boots to the network, it can request IP-related information such as the following from the server:

- an IP address
- a subnet mask
- a default gateway
- DNS and WINS server addresses

You can configure the HomeOffice Router as a DHCP server for the telecommuter's LAN.

Configuration overview

Note: Review this section completely before beginning any configuration.

1. Configure the DHCP table (see page 221).
2. Enable Dynamic IP Address Translation (DIAT for IP) on a circuit (see page 246).

How DHCP works

Note: It is unnecessary to configure the HomeOffice Router with a pool of IP addresses. The Router can generate addresses automatically based on its own Ethernet IP address.

Configure the DHCP table with a domain name and primary and secondary IP addresses of DNS and WINS servers.

Once configured, the DHCP server in the HomeOffice Router

- works in association with Dynamic IP Address Translation (DIAT for IP)

  The DHCP server operates only when DIAT is enabled on a circuit.
- can provide the following parameters to PCs on a telecommuter's local area network:

  — up to 16 IP addresses and subnet masks

  — a gateway address

  — a domain name

  — primary and secondary DNS addresses of servers on the remote network

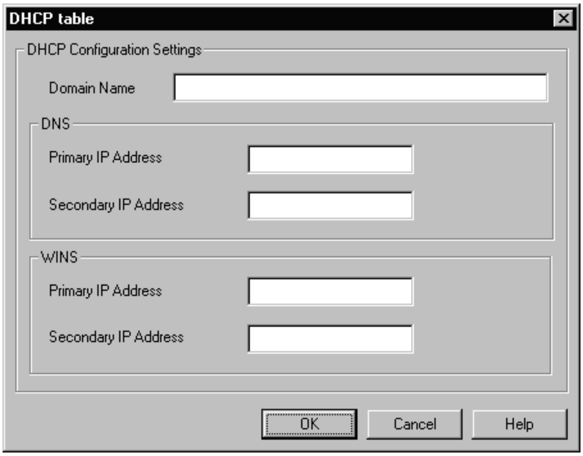
  — primary and secondary WINS addresses of servers on the remote network

To configure DHCP on the Router

1 Click the Ethernet icon.

2 Select DHCP from the pop-up menu that appears.

Result: The DHCP table screen appears.



3 Complete the fields as described in the "DHCP field descriptions" on page 222.

4 Click OK.

Result: You return to the Configuration tab.

DHCP field descriptions

Field	Description
Domain Name	Enter the name of the domain to which the HomeOffice Router belongs. For example, if your network is part of the domain called *yourcompany.com*, type **yourcompany.com**.
Primary IP Address (DNS)	Enter the IP address on the remote network of the primary domain name server.
Secondary IP Address (DNS)	Enter the IP address on the remote network of the secondary domain name server.
Primary IP Address (WINS)	Enter the IP address on the remote network of the primary Windows Internet Naming Service server.
Secondary IP Address (WINS)	Enter the IP address on the remote network of the secondary Windows Internet Naming Service server.

Routing Information Protocol

Introduction

Routing Information Protocol (RIP) is the dynamic routing protocol used on TCP/IP networks. The HomeOffice Router uses RIP over IP to exchange routing information with other routers and to update the information in its routing table.

RIP is available on both the Ethernet and ISDN interfaces. You may decide not to run RIP on the ISDN interface to reduce costs. However, you should keep RIP running on the Ethernet (LAN) interface because this does not affect connection costs.

Configuration overview

Note: Review this section completely before beginning any configuration.

To configure RIP for the Ethernet interface

Enable and configure RIP on the Ethernet interface (see page 226). RIP is enabled by default when you configure with the Install Wizard.

To configure RIP for the ISDN interface

1. Configure RIP on the ISDN interface (see page 227).
2. Configure RIP on an ISDN circuit (see page 229).

Types of RIP

Standard RIP

Normally, you use RIP on a network to pass on messages to other routers. When RIP operates in the standard way, messages are sent every 30 seconds. These messages tell the other routers that the source router is active and viable. Standard RIP uses expensive ISDN bandwidth and causes unnecessary calls on wide area networks. Standard RIP is not recommended for ISDN.

Instead of confirming availability at frequent intervals (Broadcast RIP), routing information can be configured statically in a routing table. The routing table is an adequate solution for less complex networks, but is very time-consuming for the administrator.

Triggered RIP

Triggered RIP is a method of keeping costs down on ISDN WANs. Triggered RIP is beneficial for more complex networks where the configuration can change.

When you use Triggered RIP, the Router and other devices exchange RIP information when the Router is powered up. Instead of repeating this information, the Router and other devices do not exchange packets until the configuration changes. Configuration changes trigger update messages.

Triggered RIP gives you the benefit of dynamically updating routing information without using excessive bandwidth. Update messages are sent only when the router detects a change in its routing database. This means that routing data is sent only when required, reducing ISDN usage and costs, while still being responsive to topology changes.

Note: If the ISDN address to call is set to DISABLED on a circuit, you must also support for triggered RIP, as outgoing calls cannot be made on that circuit.

When to use RIP

Use RIP when

- route selection must happen quickly to prevent network congestion (using routing tables can be time-consuming)
- you do not want to maintain routing tables

On the Ethernet interface

Use RIP on the Ethernet interface if the telecommuter has created subnets (with the use of additional routers and bridges) on his or her own network.

On the ISDN interface

Use RIP on the ISDN interface if the telecommuter’s LAN participates as an additional network (or series of subnets) recognized by the host network (DIAT is disabled). Under these circumstances, the HomeOffice Router receives regular updates on routing information by any other RIP router on the same WAN subnet.

Benefits

On the Ethernet interface

When you use RIP on the Ethernet interface

- the HomeOffice Router can exchange RIP updates with routers (if present) on the same subnet of the telecommuter’s LAN
- it is unnecessary to manually update the HomeOffice Router’s routing table

On the ISDN interface

When you use RIP on the ISDN interface

- the HomeOffice Router can exchange RIP updates with routers on the same WAN subnet of the host or central LAN
- it is unnecessary to manually update the HomeOffice Router’s routing table

Drawbacks

On the Ethernet interface

When using RIP on the Ethernet interface, there is no significant reduction in performance, regardless of whether the telecommuter’s network consists of additional subnets.

On the ISDN interface

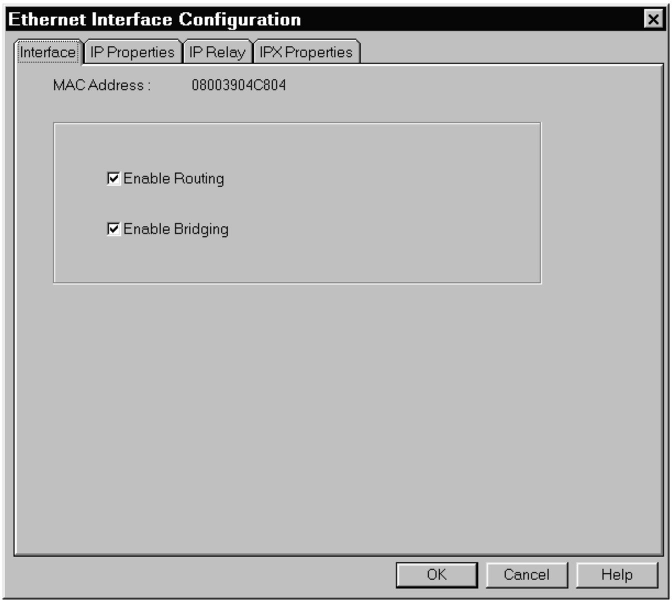
You should carefully consider RIP on the ISDN interface. The HomeOffice Router can be inundated with RIP broadcasts, which results in repeated costly activation of the ISDN circuit. If the HomeOffice Router requires only a single route to the remote access switch on the host network, a static entry for this route is recommended.

To configure RIP on the Ethernet interface

1 Click the Ethernet icon.

2 Select Properties from the pop-up menu that appears.

Result: The Ethernet Interface Configuration screen appears.



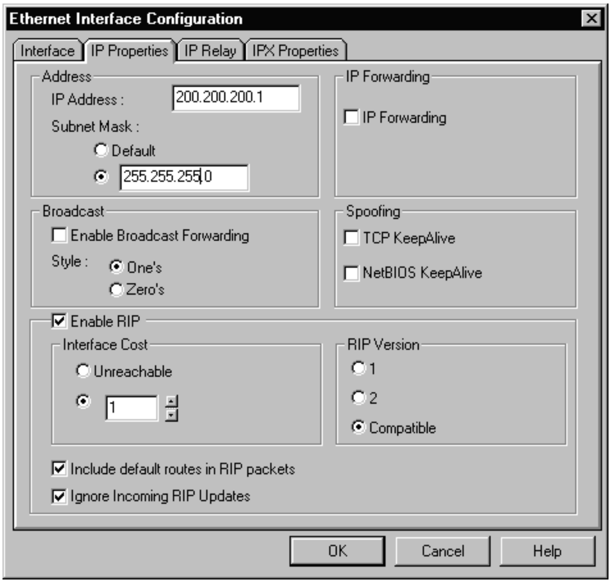
MAC Address : 08003904C804

☑ Enable Routing

☑ Enable Bridging

3 Click the IP Properties tab.

Result: The IP Properties tab appears.



Address
IP Address : 200.200.200.1
Subnet Mask :
○ Default
● 255.255.255.0

IP Forwarding
□ IP Forwarding

Broadcast
□ Enable Broadcast Forwarding
Style : ● One's ○ Zero's

Spoofing
□ TCP KeepAlive
□ NetBIOS KeepAlive

☑ Enable RIP
Interface Cost
○ Unreachable
● 1

RIP Version
○ 1
○ 2
● Compatible

☑ Include default routes in RIP packets
☑ Ignore Incoming RIP Updates

4 Click Enable RIP.

5 Complete the fields as described in the “RIP field descriptions” on page 232.

6 Click OK.

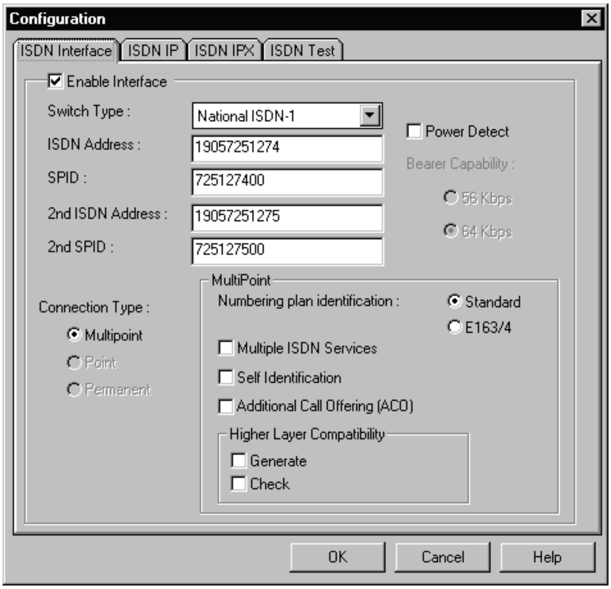
Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

To configure RIP on the ISDN interface

1 Click the ISDN icon.

2 Select Properties from the pop-up menu that appears.

Result: The Configuration screen appears.



Configuration

ISDN Interface | ISDN IP | ISDN IPX | ISDN Test

☑ Enable Interface

Switch Type : National ISDN-1

ISDN Address : 19057251274

SPID : 725127400

2nd ISDN Address : 19057251275

2nd SPID : 725127500

□ Power Detect

Bearer Capability :

○ 56 Kbps

● 64 Kbps

Connection Type :

● Multipoint

○ Point

○ Permanent

MultiPoint

Numbering plan identification : ● Standard ○ E163/4

□ Multiple ISDN Services

□ Self Identification

□ Additional Call Offering (ACO)

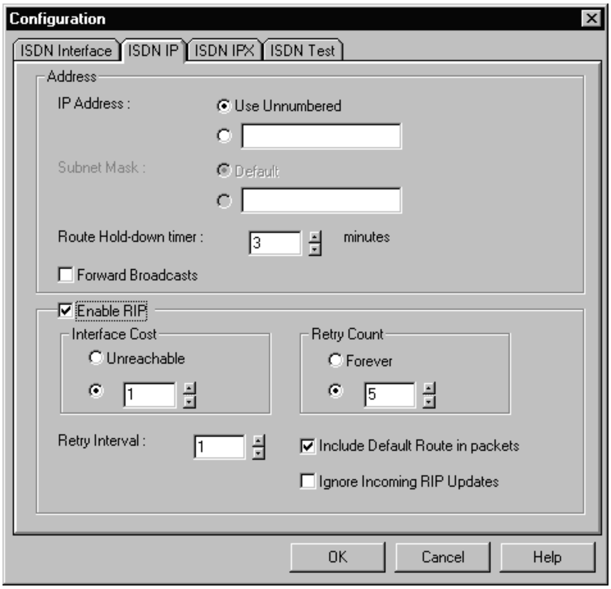
Higher Layer Compatibility

□ Generate

□ Check

3 Click the ISDN IP tab.

Result: The ISDN IP tab appears.



Configuration

ISDN Interface | ISDN IP | ISDN IPX | ISDN Test

Address

IP Address : ● Use Unnumbered

○

Subnet Mask : ● Default

○

Route Hold-down timer : 3 minutes

□ Forward Broadcasts

☑ Enable RIP

Interface Cost

○ Unreachable

● 1

Retry Count

○ Forever

● 5

Retry Interval : 1

☑ Include Default Route in packets

□ Ignore Incoming RIP Updates

4 Click Enable RIP.

5 Complete the fields as described in the “RIP field descriptions” on page 232.

6 Click OK.

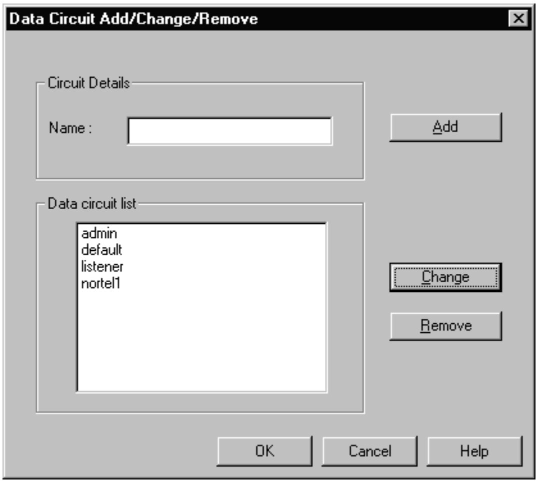
Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

To configure RIP on an ISDN circuit

1 Click the ISDN icon.

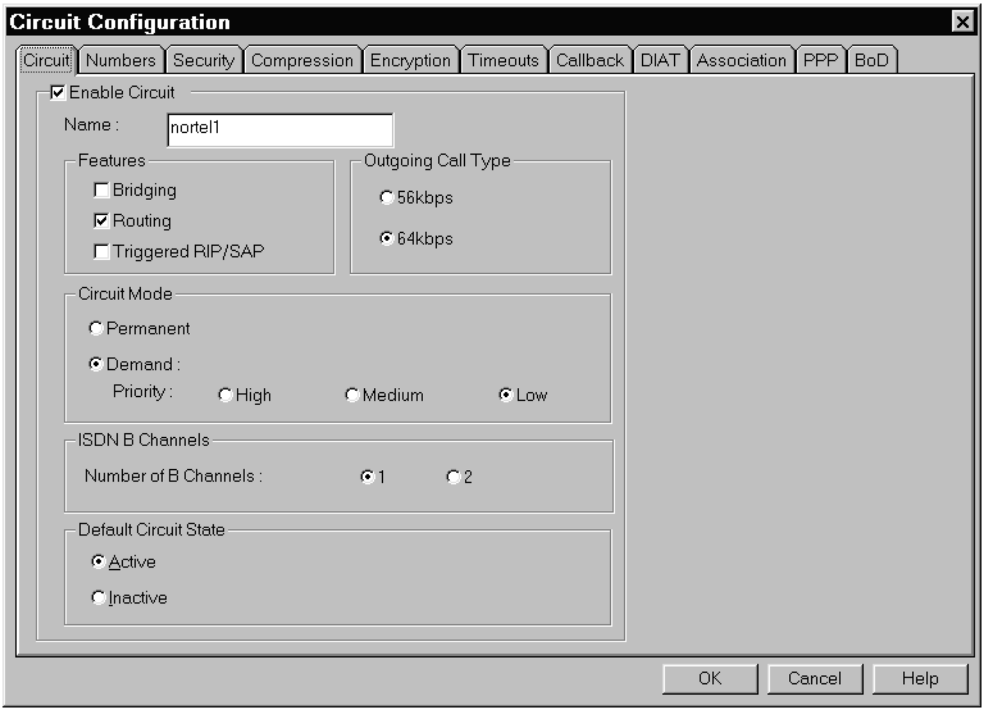
2 Select Circuits from the pop-up menu that appears.

Result: The Data Circuit Add/Change/Remove screen appears.



3 Select the circuit for which you want to configure RIP, and then click Change.

Result: The Circuit Configuration screen appears.



Circuit Configuration

☑ Enable Circuit

Name : nortel1

Features

☐ Bridging

☑ Routing

☐ Triggered RIP/SAP

Outgoing Call Type

○ 56kbps

● 64kbps

Circuit Mode

○ Permanent

● Demand :

Priority : ○ High ○ Medium ● Low

ISDN B Channels

Number of B Channels : ● 1 ○ 2

Default Circuit State

● Active

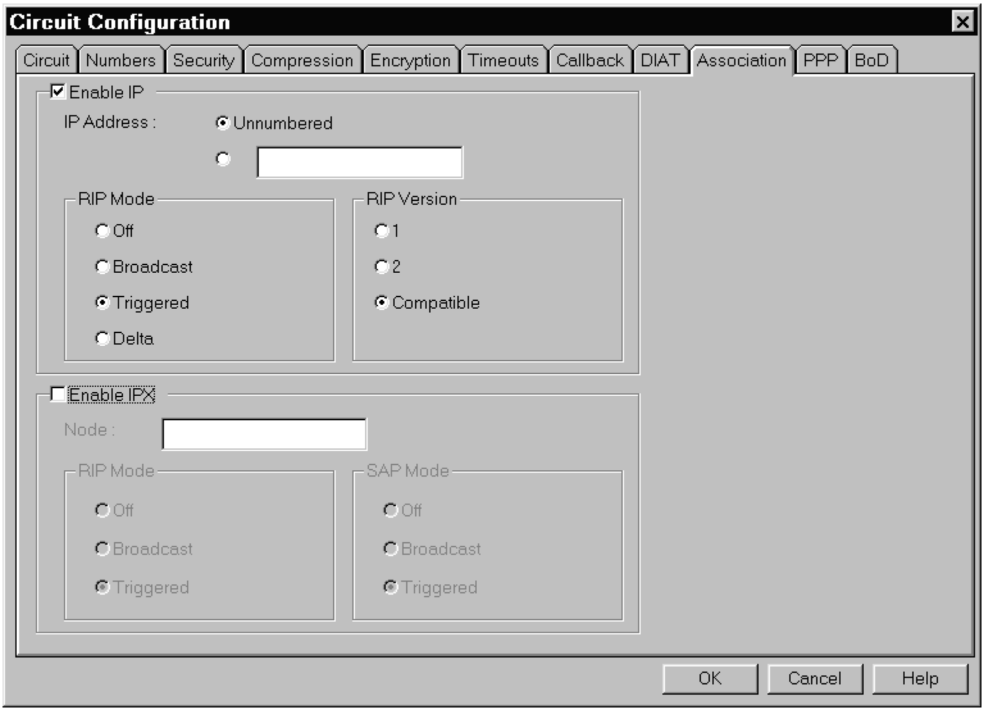
○ Inactive

4 If you want to use Triggered RIP on this circuit, ensure that the Triggered RIP/SAP option is selected.

Note: You must enable Triggered RIP and SAP if you are using multiple static routes.

5 Click the Association tab.

Result: The Association tab appears.



☑ Enable IP

IP Address : ● Unnumbered ○

RIP Mode: ○ Off ○ Broadcast ● Triggered ○ Delta

RIP Version: ○ 1 ○ 2 ● Compatible

□ Enable IPX

Node :

RIP Mode: ○ Off ○ Broadcast ● Triggered

SAP Mode: ○ Off ○ Broadcast ● Triggered

6 Complete the RIP Mode and RIP Version fields as described in “RIP field descriptions” on page 232.

7 Click OK.

Result: The Data Circuit Add/Change/Remove screen appears.

8 Click OK again.

Result: You return to the Configuration tab.

RIP field descriptions

Field	Where	Description
Interface cost	Ethernet interface ISDN interface	This is the notional cost of using RIP with IP. If there are several routes to a destination, the Router chooses the one with the lowest interface cost. If an interface gives access to a particularly expensive WAN, set the parameter quite high. If you want to force traffic to use a particular route, set the value quite low. The interface cost should normally be set to 1. However, there can be more than one route to a destination. If the cost of using this route is greater than the cost for another route, then you should set the cost to a value greater than 1. This indicates that you should choose the other cheaper route in preference to this one. If you select Unreachable, this prevents all of the RIP routes from being learned from this interface.
RIP Mode	ISDN circuit (Association tab)	In general, use Triggered over an ISDN connection because this setting affects only this circuit, not the entire interface. About RIP Modes • Off: RIP is off for the circuit, so you must create static routes. Use the IP Routing table to do this. • Broadcast: RIP messages are sent every 30 seconds. If the link is not up, the link opens for these messages. • Triggered: RIP messages are sent only when the Routing table changes. If the link is not up, the link opens for these messages.

Field	Where	Description
RIP Mode (continued)	ISDN circuit (Association tab)	• Delta: RIP messages are sent only when the link is already up for other reasons. If the link is not up, these messages are not sent. This reduces traffic and connection costs. **Note:** If you are connecting to an Intel Shiva LanRover Access Switch, select Delta for the most efficient, cost-effective connection.
RIP Version	Ethernet interface ISDN circuit (Association tab)	The HomeOffice Router supports different RIP versions to allow enhanced compatibility with other routers. The following list summarizes the features of each version: • 1: does not include subnet information Choose RIP Version 1 if you are connecting to a small network without subnets or you are connecting to a network that is also using RIP Version 1. • 2: includes subnet information Choose RIP Version 2 if you are connecting to a large network that is subnetted, or if you know that the remote network is also using RIP Version 2. **Note:** RIP Versions 1 and 2 can run in Triggered or Broadcast mode. • Compatible: Version 2 is backwards-compatible with Version 1 Choose Compatible if you do not know which RIP version that the remote network is running.

Field	Where	Description
RIP Version (continued)	Ethernet interface ISDN circuit (Association tab)	If you are not sure of which version to use, ask the network administrator of the network concerned. If you choose RIP Version 2, you do not need to set up static routes from the remote access switch to the HomeOffice Router. **Note:** The remote access switch on the remote network must also be running RIP Version 2.
Retry count	ISDN interface	The triggered retry count defines the number of times that RIP tries to connect with RIP on the destination router if the Router cannot communicate (for example, if communications fail). Click Forever, or enter a value between 0 and 99. The recommended value is 5.
Retry interval	ISDN interface	The triggered retry interval defines the interval in minutes between triggered retry attempts. Enter a value between 1 and 10.
Include default routes in RIP packets	Ethernet interface ISDN interface	The default route is the route to the remote network over the circuit that you specified with the Install Wizard.
Ignore Incoming RIP Updates	Ethernet interface ISDN interface	Select this option if you are on a large network. When you select this option, the HomeOffice Router sends out routing information about itself but does not receive routing information. This reduces the number of routes that need to be stored in the HomeOffice Router’s routing table.

Unnumbered links

Introduction

You can set ISDN IP addresses on your Router to be *unnumbered*. By doing this, you can route IP over a link between two devices without assigning an IP address to the ISDN interfaces. This allows you to save valuable IP address space.

Note: If you want to configure the IP address for the ISDN interface, this implies that you want to create a numbered link to the wide area network (WAN). For instructions on creating a numbered link, see “IP address and subnet mask” on page 201.

Configuration overview

Note: Review this section completely before beginning any configuration.

1. Enable unnumbered links on the ISDN interface (see page 237).
2. Enable IP and unnumbered links on a circuit (see page 238).
3. Add a route to the IP Routes table (see page 240).

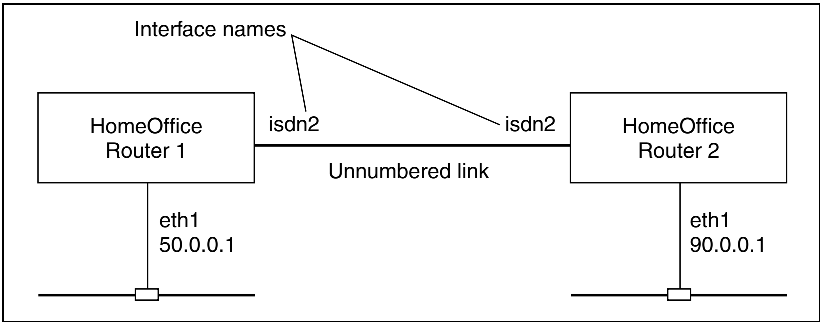
When to use an unnumbered link

The unnumbered link option allows the HomeOffice Router to be another recognized routing device extending off the main host network. The HomeOffice Router may provide connectivity to another subnetted LAN within the telecommuter’s Ethernet network. Under this circumstance, the Router is configured with static (or dynamic) addresses to route data between the LANs and pass routing information (RIP) in a similar manner to a conventional network router.

Example

In the following illustration, there is an unnumbered link between HomeOffice Router 1 and HomeOffice Router 2. These two devices can still communicate with each other, although neither of the WAN interfaces has been assigned an IP address. Instead, a route is assigned between a device and its destination network, using interfaces and circuits instead of IP addresses.

ISG623_I



Benefits

By using unnumbered links, you conserve IP address space on the central host DHCP server.

Drawbacks

When unnumbered links are used, the ISDN interface is not recognized by any TCP/IP utilities that require an IP address such as ping, Telnet, Tracert, and so on. The interface is transparent to these commands.

Using ping or Telnet

If you set an address to be unnumbered, you cannot ping that interface or Telnet to it.

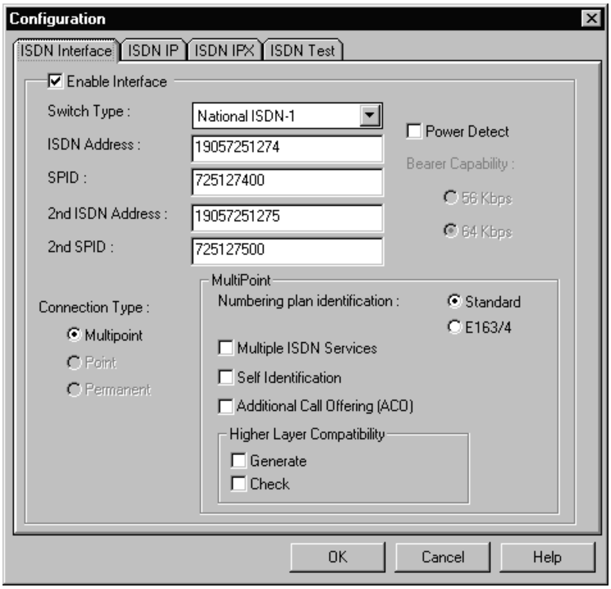
You can ping or Telnet to the Ethernet interface. You cannot set unnumbered IP addresses on Ethernet interfaces or on bridging-only interfaces.

To enable unnumbered links on the ISDN interface

1 Click the ISDN icon.

2 Select Properties from the pop-up menu that appears.

Result: The Configuration screen appears.



☑ Enable Interface

Switch Type : National ISDN-1

ISDN Address : 19057251274

SPID : 725127400

2nd ISDN Address : 19057251275

2nd SPID : 725127500

□ Power Detect

Bearer Capability :

○ 56 Kbps

● 64 Kbps

Connection Type :

● Multipoint

○ Point

○ Permanent

MultiPoint

Numbering plan identification : ● Standard ○ E163/4

□ Multiple ISDN Services

□ Self Identification

□ Additional Call Offering (ACO)

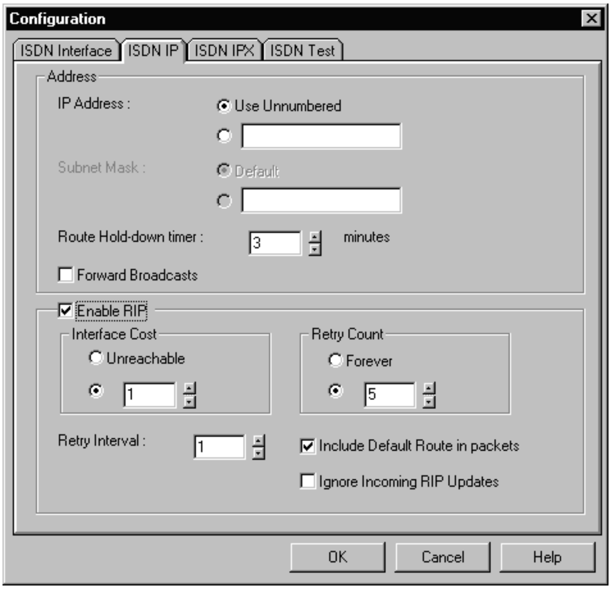
Higher Layer Compatibility

□ Generate

□ Check

3 Click the ISDN IP tab.

Result: The ISDN IP tab appears.



Address

IP Address : ● Use Unnumbered ○

Subnet Mask : ● Default ○

Route Hold-down timer : 3 minutes

□ Forward Broadcasts

☑ Enable RIP

Interface Cost: ○ Unreachable ● 1

Retry Count: ○ Forever ● 5

Retry Interval : 1

☑ Include Default Route in packets

□ Ignore Incoming RIP Updates

4 Click Use Unnumbered.

5 Click OK.

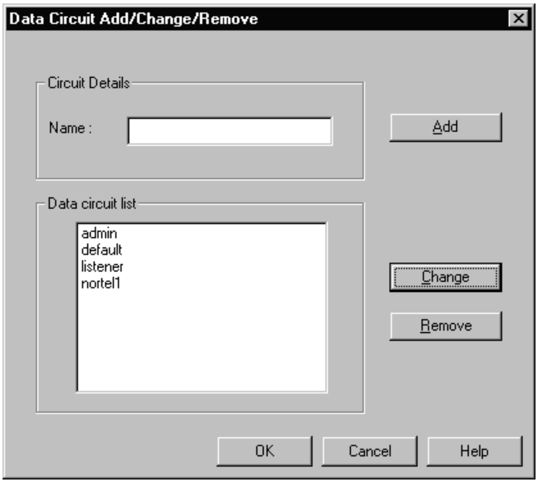
Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

To enable IP and unnumbered links on a circuit

1 Click the ISDN icon.

2 Select Circuits from the pop-up menu that appears.

Result: The Data Circuit Add/Change/Remove screen appears.



Data Circuit Add/Change/Remove

Circuit Details

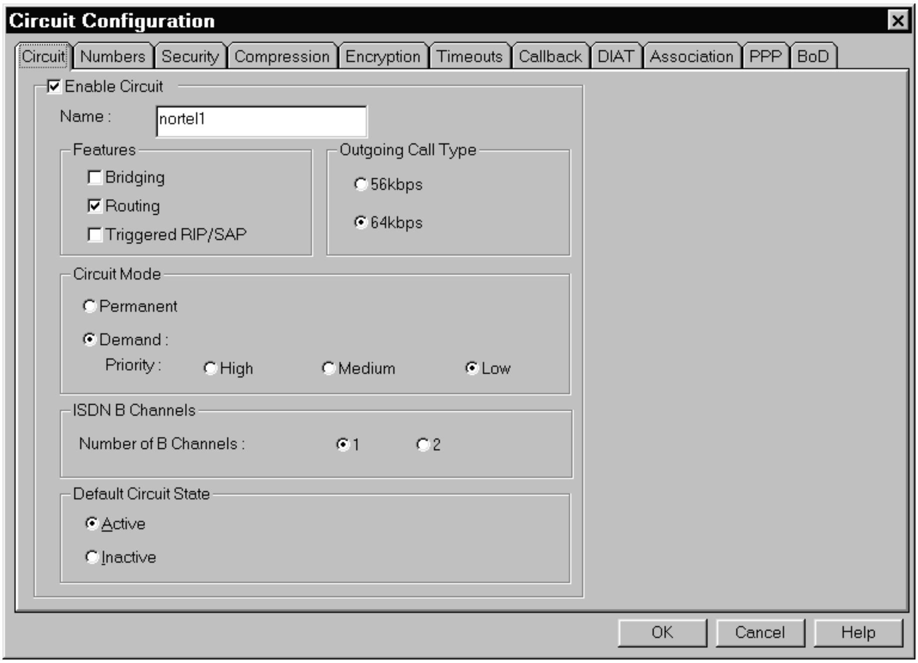
Name :

Data circuit list

admin
default
listener
nortel1

3 Select the circuit for which you want to configure the unnumbered link, and then click Change.

Result: The Circuit Configuration screen appears.



Circuit Configuration

☑ Enable Circuit

Name : nortel1

Features

□ Bridging
☑ Routing
□ Triggered RIP/SAP

Outgoing Call Type

○ 56kbps
● 64kbps

Circuit Mode

○ Permanent
● Demand :
Priority : ○ High ○ Medium ● Low

ISDN B Channels

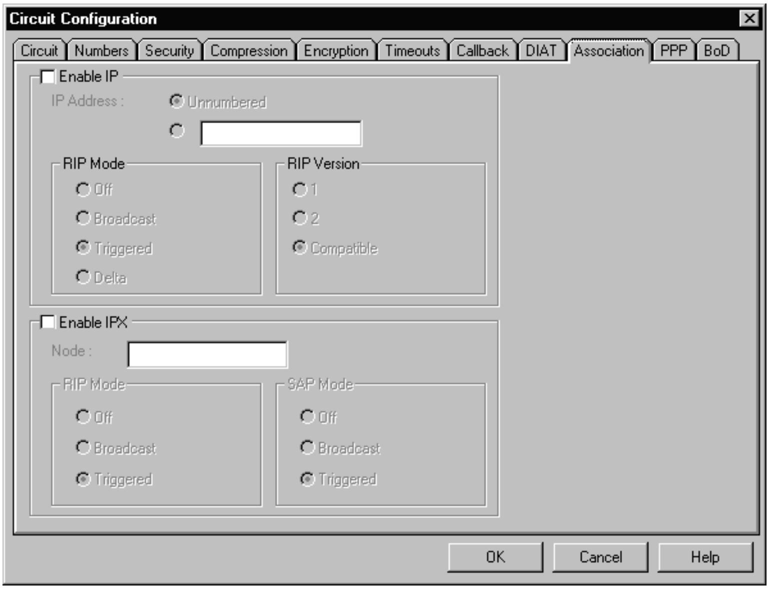
Number of B Channels : ● 1 ○ 2

Default Circuit State

● Active
○ Inactive

4 Click the Association tab.

Result: The Association tab appears.



□ Enable IP

IP Address : ● Unnumbered
○

RIP Mode
○ Off
○ Broadcast
● Triggered
○ Delta

RIP Version
○ 1
○ 2
● Compatible

□ Enable IPX

Node :

RIP Mode
○ Off
○ Broadcast
● Triggered

SAP Mode
○ Off
○ Broadcast
● Triggered

5 Ensure that Enable IP is checked.

6 Click Unnumbered.

7 Click OK.

Result: The Data Circuit Add/Change/Remove screen appears.

8 Click OK again.

Result: You return to the Configuration tab.

To add a route to the IP Routes table

For instructions on adding a route to the IP Routes table, see “To create IP routes” on page 217.

Dynamic IP Address Translation

Introduction

Dynamic IP Address Translation (DIAT for IP) is a mechanism by which a remote network of one or more devices can appear as a single dial-in user to the host network. This allows the remote network the flexibility to implement an addressing scheme that is invisible to the host network.

DIAT for IP is a form of Network Address Translation (NAT) used on other vendors' routers.

Configuration overview

Note: Review this section completely before beginning any configuration.

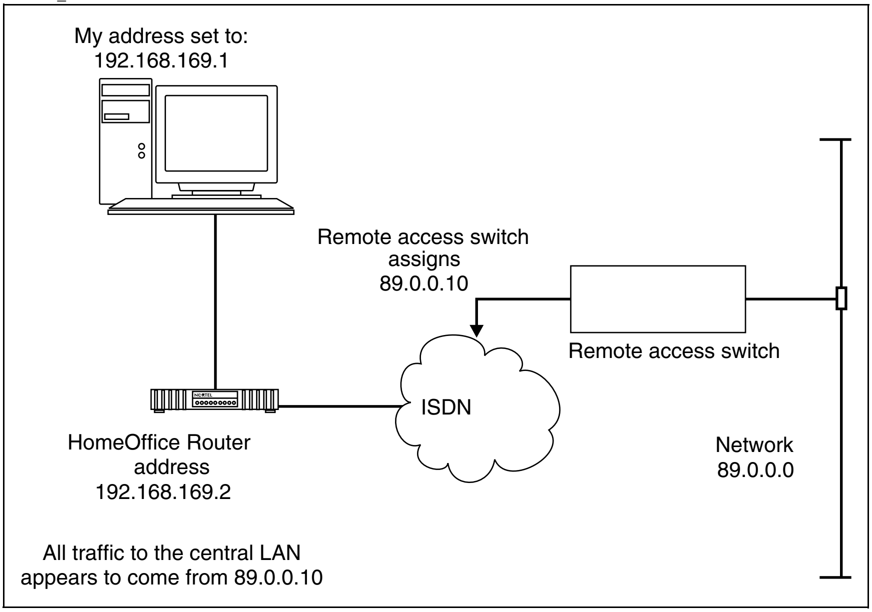
1. Enable DIAT for IP on the ISDN circuit as either single-host or multi-host (see page 246).
2. If Multi Host is enabled on a circuit, configure the DIAT for IP table on the Ethernet interface (see page 248).

How DIAT for IP works

Single-host DIAT for IP

In the illustration that follows, the corporate office network is 89.0.0.0. When a telecommuter connects to the corporate office network, the telecommuter's local network is given the IP address 89.0.0.10, regardless of the IP addresses that have already been assigned to the local network. This IP address is used to communicate with the corporate office network, regardless of which computer is connecting from the telecommuter's local network. This makes the telecommuter's local network appear as a single device on the corporate office network. See the following diagram.

ISG617_i

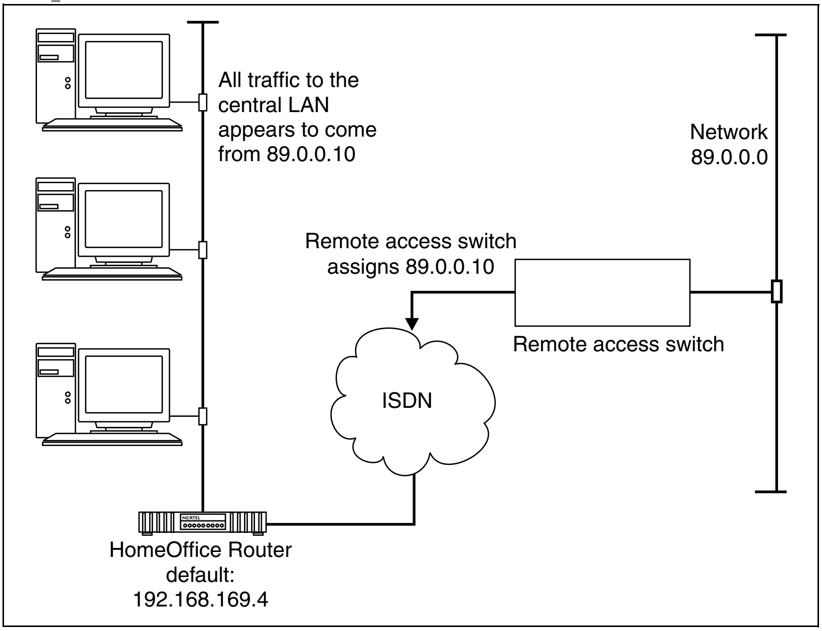

My address set to:
192.168.169.1
Remote access switch assigns 89.0.0.10
Remote access switch
ISDN
NORTEL
HomeOffice Router address 192.168.169.2
Network 89.0.0.0
All traffic to the central LAN appears to come from 89.0.0.10

Multi-host DIAT for IP

When two or more hosts share an IP address with the HomeOffice Router, this is known as multi-host DIAT for IP. With multi-host DIAT for IP, the HomeOffice Router provides TCP Port Translation (as well as IP Address Translation). This ensures that packets are returned to the correct device. The remote LAN still appears as a single device to the central site. See the following illustration.

A key advantage of multi-host DIAT for IP is that all of the remote sites can be given the same configuration by a network manager.

ISG611_I


All traffic to the central LAN appears to come from 89.0.0.10
Network 89.0.0.0
Remote access switch assigns 89.0.0.10
Remote access switch
ISDN
NORTEL
HomeOffice Router default: 192.168.169.4

DIAT for IP features

DIAT for IP provides the following features:

- dynamic address discovery

  A network address for the telecommuter is obtained from the IP-based host network and assigned to the HomeOffice Router.

- address translation

  The source address of outbound data from a remote network device is translated to the address of the HomeOffice Router. To the host network, any data that originates from a device on the remote network appears as if it originates from the HomeOffice Router.

  Conversely, data from the host network that is destined for a remote device is given the address of the HomeOffice Router. The HomeOffice Router translates this address to the remote network address of the destination device and routes the data.

  The address translation that occurs is transparent to both the remote and host networks.

- port translation for remote networks with multiple devices

  TCP port translation ensures that packets are routed to the correct remote device.

Benefits

DIAT for IP provides the following significant benefits:

- You can use IP and IPX on the same circuit, provided that both are set for DIAT or for LAN-to-LAN.
- When using DIAT for IP, the HomeOffice Router can fully participate in very large, corporate IP networks.
- IP addresses from the central host address pool are not required for devices on the telecommuter’s network. You conserve valuable IP address space.
- Remote network addressing is flexible.
- Telecommuters can use any addressing scheme on their local networks. The telecommuter’s network is *invisible* to the central host LAN.

Drawbacks

Some e-mail packages, calendar scheduling software, or other applications may not work with DIAT for IP. If you are using such applications, do not enable DIAT for IP.

If more than ten hosts share an IP address, this can cause a degradation in performance due to ISDN bandwidth limitations.

Another disadvantage of multi-host DIAT for IP is that if you are using a UDP port-specific application, only one device can use that UDP port at any given time. This is a limitation of IP.

When to use DIAT for IP

Enable DIAT for IP on the HomeOffice Router when DHCP is used to assign IP addresses to telecommuters.

DIAT table

When you invoke an application, such as a web browser, FTP client, or Telnet program to connect to a service on a host (WWW, FTP, Telnet), you establish a session. A session is a connection to a service on a service host.

The DIAT table stores service port numbers and IP address information about different hosts on the network (for example, printer, Telnet, web services, mail services, and FTP). You can configure the HomeOffice Router with a DIAT table of local services and the local address of the device supporting these services. The HomeOffice Router uses the information in its DIAT table to direct incoming sessions to the appropriate host on its network. This allows local services to be exported without the remote site having to know the local IP address.

Common services

Some common services (for example, Telnet) use a widely recognized port number. The HomeOffice Router already knows the most common service port numbers as indicated in the following table:

Service	Port number
FTP	21
News	515
SMTP	25
Telnet	23
TFTP	69
HTTP (WWW)	80

Less common services

Other services, such as Network Time Protocol (NTP), are not as common. They do not use widely recognized port numbers. For less common services, you must enter a port number as well as the IP address of the device on which the service is located.

DIAT table and security

The DIAT table can act as an additional security feature. This is because you can direct incoming services to specific host IP addresses. For example, if you have a firewall, you can direct all incoming services to it.

When to configure the DIAT table

Configure the DIAT table only if multi-host DIAT for IP is enabled on a circuit.

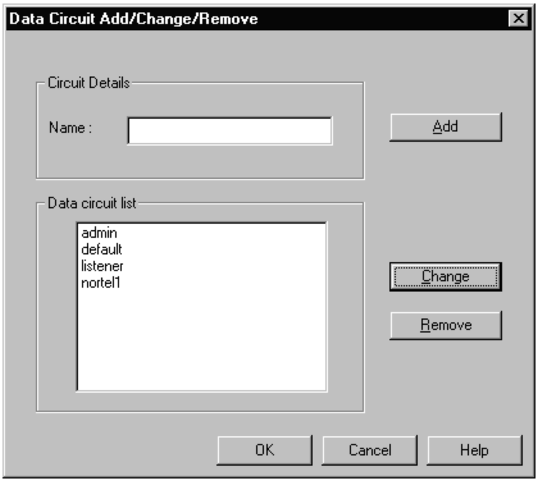
To enable DIAT on a circuit

Note: You can perform this procedure on a circuit that is not being used (such as the admin circuit).

1 Click the ISDN icon.

2 Select Circuits from the pop-up menu that appears.

Result: The Data Circuit Add/Change/Remove screen appears.



Data Circuit Add/Change/Remove

Circuit Details

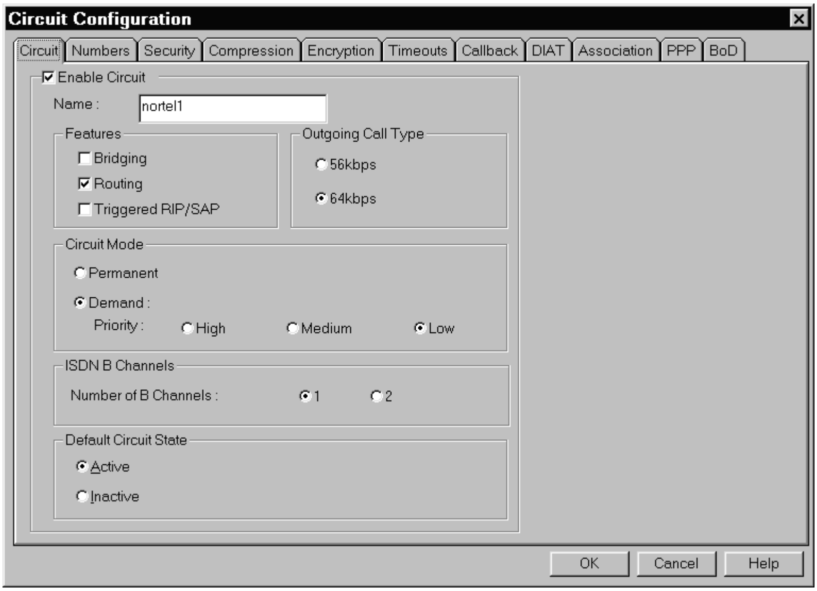
Name :

Data circuit list

admin
default
listener
nortel1

3 Select the circuit for which you want to enable DIAT for IP, and then click Change.

Result: The Circuit Configuration screen appears.



☑ Enable Circuit

Name : nortel1

Features

□ Bridging

☑ Routing

□ Triggered RIP/SAP

Outgoing Call Type

○ 56kbps

● 64kbps

Circuit Mode

○ Permanent

● Demand :

Priority : ○ High ○ Medium ● Low

ISDN B Channels

Number of B Channels : ● 1 ○ 2

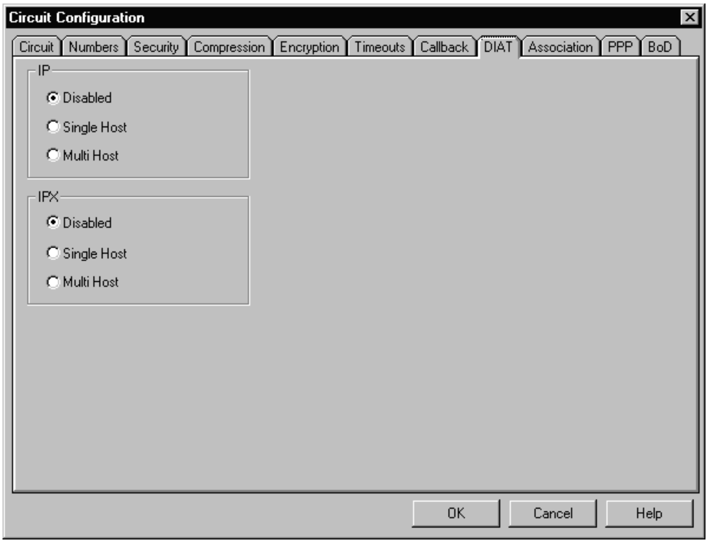
Default Circuit State

● Active

○ Inactive

4 Click the DIAT tab.

Result: The DIAT tab appears.



IP

● Disabled

○ Single Host

○ Multi Host

IPX

● Disabled

○ Single Host

○ Multi Host

5 In the IP area, do one of the following:

- Click Single Host if only the PC will be sharing an IP address with the HomeOffice Router.
- Click Multi Host if the PC and one or more other devices will be sharing an IP address with the HomeOffice Router.

6 Click OK.

Result: The Data Circuit Add/Change/Remove screen appears.

7 Click OK again.

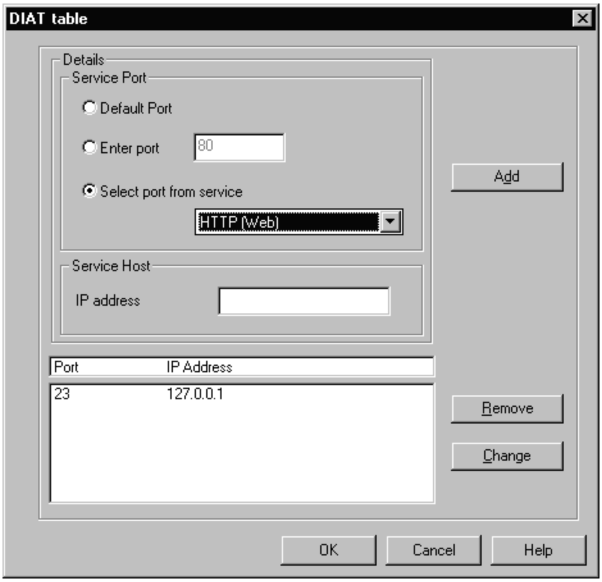
Result: You return to the Configuration tab.

To configure the DIAT table

1 Click the Ethernet icon.

2 Select DIAT table from the pop-up menu that appears.

Result: The DIAT table screen appears.



DIAT table

Details

Service Port

○ Default Port

○ Enter port 80

● Select port from service

HTTP (Web)

Service Host

IP address

Port	IP Address
23	127.0.0.1

3 Complete the fields as described in “DIAT table field descriptions” on page 249.

4 Click Add.

Result: The service is added to the table at the bottom of the screen.

5 When you have added all the services required, click OK.

Result: You return to the Configuration tab.

DIAT table field descriptions

Field	Description
Default Port	Select this option if you want to direct all incoming sessions to one host only. Then enter the IP address of that host.
Enter port	Select this option if you want to configure a port for services that are not common. Then enter the port number. **Notes:** • If you select a service from the Select port from service list box, then the port number appears in this field. • If you do not enter port information in the DIAT table, then incoming data packets may be blocked.
Select port from service	Select this option if you want to create entries for common types of sessions. Then select the type of service from the list box. **Note:** The port number for the selected service appears in the Enter port field.
Service Host IP address	Enter the IP address of the service host (on the HomeOffice Router's LAN) to which incoming sessions are to be directed. **Note:** If you selected Default Port, all incoming sessions are directed to this IP address.

IP Forwarding

Introduction

When DIAT for IP is enabled, you can use a single PC with any IP address to gain network connectivity. You can use IP Forwarding with DIAT for IP so that the HomeOffice Router can forward the PC's requests. With DIAT for IP and IP Forwarding enabled, a telecommuter can have the same configuration both at home and in the office.

Configuration overview

Note: Review this section completely before beginning any configuration.

1. Enable DIAT for IP on the ISDN circuit as either Single Host or Multi Host (see page 246).
2. Enable IP Forwarding on the Ethernet interface (see page 252).

When to use IP Forwarding

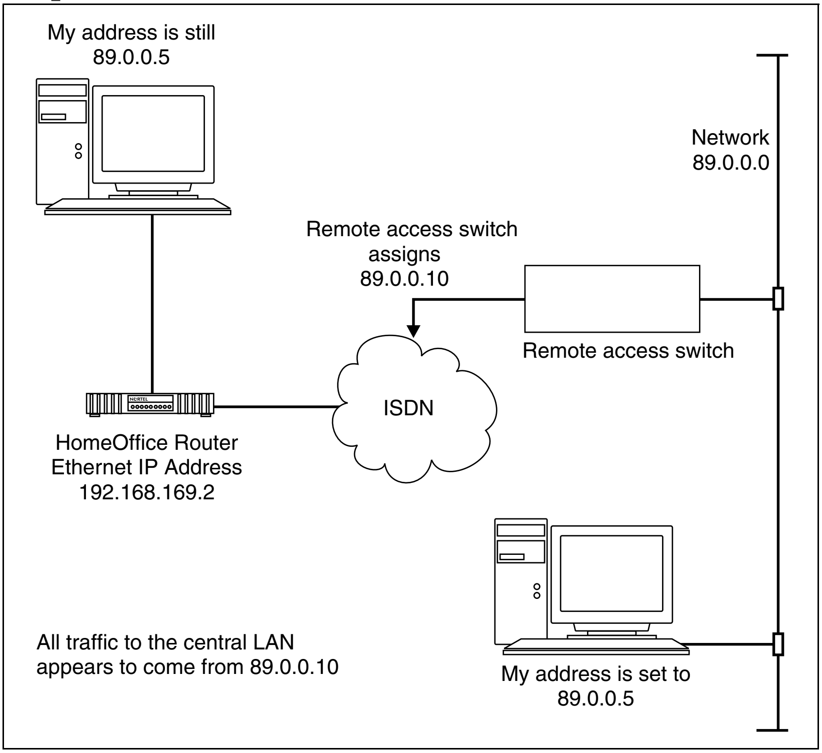
Select IP Forwarding if

- telecommuters want to use their laptop computers at home and in the office without changing IP addresses
- HomeOffice Routers are configured for Single Host DIAT for IP

How DIAT for IP works with IP Forwarding

By using IP Forwarding, the telecommuter with an IP address of 89.0.0.5 at the central site can take the laptop computer home and use it there without changing its IP address. The HomeOffice Router accepts packets from the laptop computer connected to its LAN, and forwards these onto the central LAN using address translation. The HomeOffice Router also proxies ARP and acts as the default router, regardless of what address the default router is configured as on the laptop computer.

ISG614_I



Benefits

There are two situations in which DIAT for IP with IP Forwarding can be useful:

- Telecommuters can have a single IP address configuration for the PC at home and in the office.
- Network managers must maintain and support only one boot option.

Drawbacks

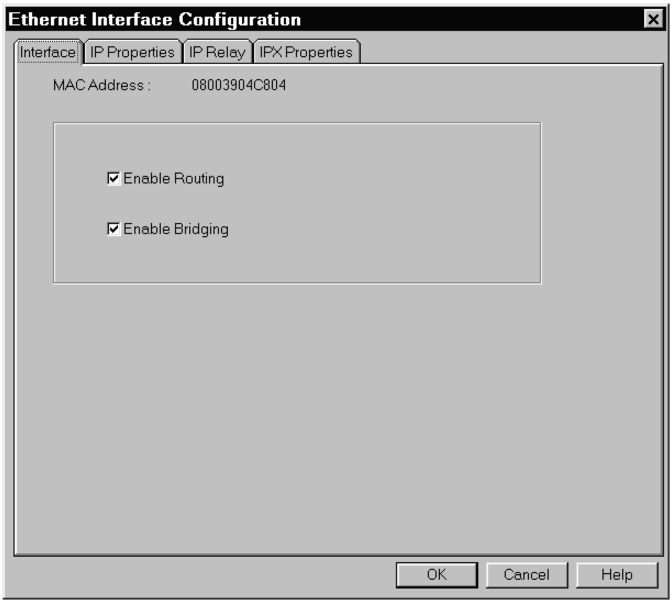
When you use IP Forwarding, you cannot use the configuration backup, configuration restore, and upgrade functions in Local Manager from the PC connected by Ethernet to the HomeOffice Router. However, you can perform these functions by accessing HomeOffice Router remotely over an ISDN connection.

To enable IP Forwarding on the Ethernet interface

1 Click the Ethernet icon.

2 Select Properties from the pop-up menu that appears.

Result: The Ethernet Interface Configuration screen appears.



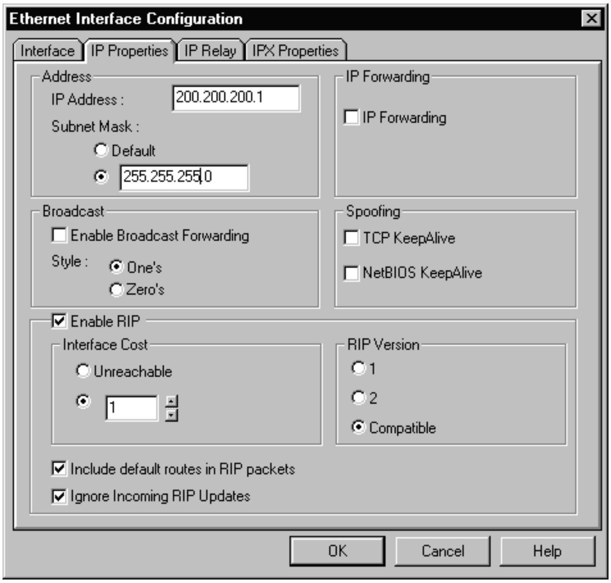
MAC Address : 08003904C804

☑ Enable Routing

☑ Enable Bridging

3 Click the IP Properties tab.

Result: The IP Properties tab appears.



Address

IP Address : 200.200.200.1

Subnet Mask :

○ Default

● 255.255.255.0

IP Forwarding

☐ IP Forwarding

Broadcast

☐ Enable Broadcast Forwarding

Style : ● One's ○ Zero's

Spoofing

☐ TCP KeepAlive

☐ NetBIOS KeepAlive

☑ Enable RIP

Interface Cost

○ Unreachable

● 1

RIP Version

○ 1

○ 2

● Compatible

☑ Include default routes in RIP packets

☑ Ignore Incoming RIP Updates

4 Ensure that the IP Forwarding check box contains a check mark.

5 Ensure that the IP address shown in the IP Address field is on a different network than the PC to which the Router is connected.

6 Click OK.

Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

Broadcast Forwarding and IP Relay

Introduction

A broadcast is a network transaction that sends data to one or more hosts connected to the network. The addresses to which the broadcast is being sent may be the broadcast addresses of a remote IP network or the IP address of a server itself.

Forwarding is the process by which the Router sends requests from a server on its network to another server on the same or other network. Forwarding is completed according to entries in the Router's IP Relay table.

Note: You often need Broadcast Forwarding in Windows NT and BootP environments.

Configuration overview

Note: Review this section completely before beginning any configuration.

1. Enable Broadcast Forwarding on the Ethernet interface (see page 257).
2. Enable Broadcast Forwarding on the ISDN interface (see page 259).
3. Configure the IP Relay table (see page 260).

What you can broadcast

You can forward BootP and DHCP packets, NetBIOS packets, or all of the UDP packets. You can specify which packet types to forward or you can select all three of them.

IP Relay table

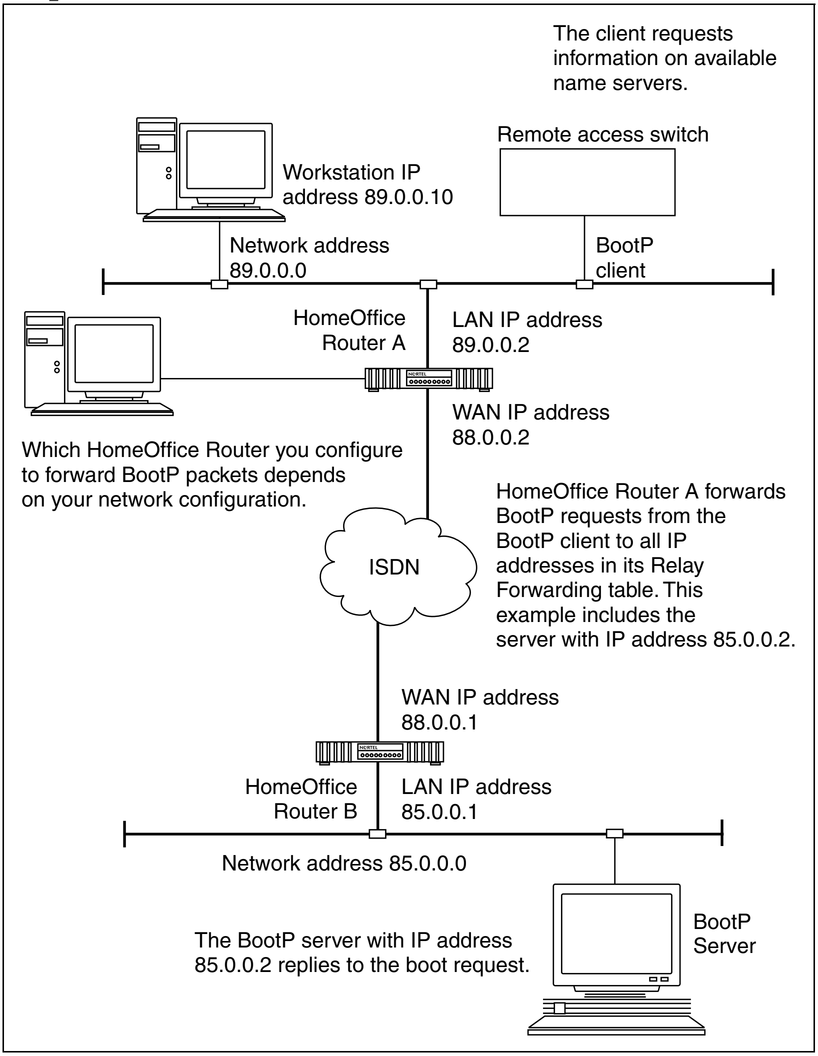
You can configure the Router to send UDP broadcasts over IP by specifying up to 16 broadcast destinations in the IP Relay table. The Router then routes broadcasts from the local network to the specified destinations.

Configure the IP Relay table if you are using the Router to connect networks. If telecommuters use HomeOffice Routers, the IP Relay table is not required.

How Broadcast Forwarding works

The following illustration shows a terminal or PC attached to a HomeOffice Router. This indicates the unit that is being configured. The diagram also indicates the addressing information that is needed.

ISG622_I


The client requests information on available name servers.
Remote access switch
Workstation IP address 89.0.0.10
Network address 89.0.0.0
BootP client
HomeOffice Router A
LAN IP address 89.0.0.2
WAN IP address 88.0.0.2
Which HomeOffice Router you configure to forward BootP packets depends on your network configuration.
HomeOffice Router A forwards BootP requests from the BootP client to all IP addresses in its Relay Forwarding table. This example includes the server with IP address 85.0.0.2.
ISDN
WAN IP address 88.0.0.1
HomeOffice Router B
LAN IP address 85.0.0.1
Network address 85.0.0.0
The BootP server with IP address 85.0.0.2 replies to the boot request.
BootP Server

Some NetBIOS/IP, BootP, and DHCP implementations are limited in the way that they treat NetBIOS, BootP, and DHCP broadcasts. For example, if a BootP client sends a BootP request to 89.255.255.255, normal IP rules mean that this broadcast is restricted to network 89.0.0.0. If the server on network 85 holds the booting information for the BootP client on network 89.0.0.0, the BootP client cannot boot.

To avoid this problem, you can configure the Router with up to 16 IP addresses to which received BootP requests should be sent. These addresses can be the broadcast address of a remote IP network or the IP address of a server itself. These addresses are stored in the Router’s IP Relay table. All of the BootP request broadcasts are then forwarded by your device to the named IP addresses.

Broadcast style

The broadcast style defines the address format for IP broadcasts over the LAN. It can be ones or zeros:

- Ones: The style for IP broadcasts over the LAN is similar to the following example: 89.255.255.255.

  Note: Normally, you should select ones.
- Zeros: The broadcast style is similar to 89.0.0.0.

  Note: This style is no longer used except for older networks. Ones are the standard.

DHCP packets

Your device also supports the forwarding of Dynamic Host Configuration Protocol (DHCP) packets. This allows the client PC to find its own address configuration details from a central DHCP server. In certain networking environments, such as Microsoft Windows NT, individual computers or clients can extract their configuration from a server. This reduces the effort required to administer the network.

The previous illustration, which shows BootP operation using the HomeOffice Router, there is a BootP client on one site and a BootP server on the other. In a configuration like this, you must only set up the HomeOffice Router on the client site to forward BootP, NetBIOS, and DHCP broadcasts as appropriate.

If there is a BootP, NetBIOS, or DHCP server on both sites, you must set up the devices on both ends of the link.

Benefits

Broadcast Forwarding

- provides IP address portability between home and office
- reduces the need to maintain multiple configurations on a laptop computer
- provides telecommuters with access to central host WINS and DNS servers

Drawbacks

Broadcast Forwarding

When you forward all of the UDP broadcasts, you can keep ISDN links open unnecessarily.

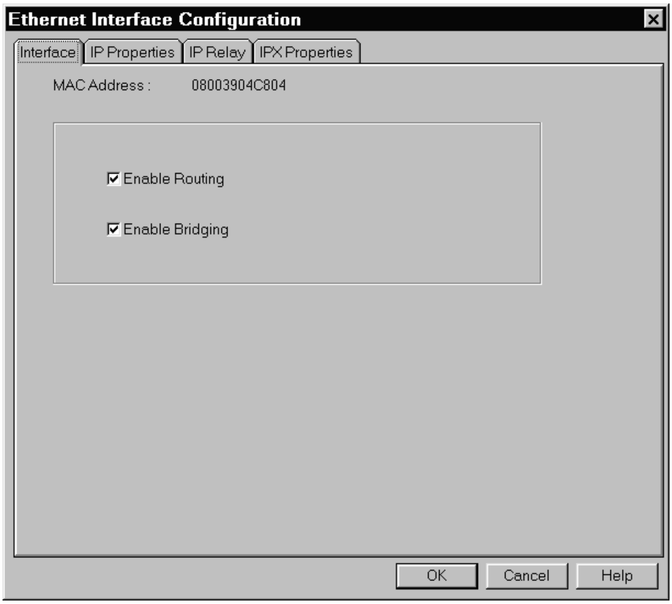
IP Relay table

If you use the IP Relay table with WINS, you increase ISDN line usage.

To enable Broadcast Forwarding on the Ethernet interface

1. Click the Ethernet icon.
2. Select Properties from the pop-up menu that appears.

   Result: The Ethernet Interface Configuration screen appears.



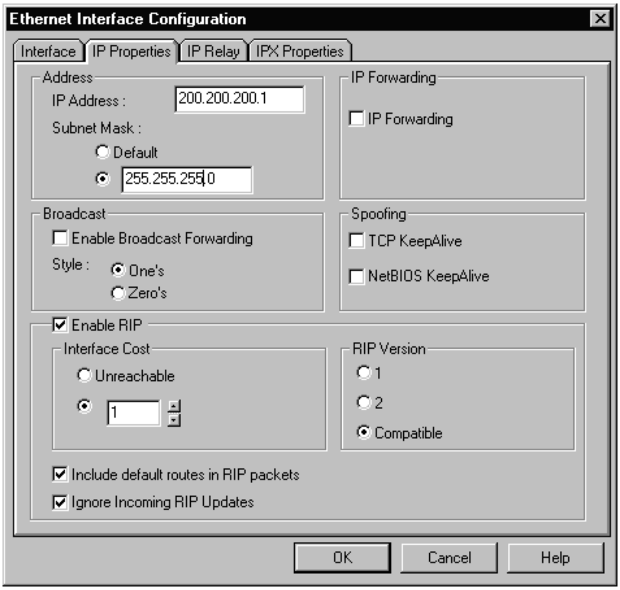
MAC Address : 08003904C804

☑ Enable Routing

☑ Enable Bridging

3 Click the IP Properties tab.

Result: The IP Properties tab appears.



Address

IP Address : 200.200.200.1

Subnet Mask :

○ Default

● 255.255.255.0

IP Forwarding

□ IP Forwarding

Broadcast

□ Enable Broadcast Forwarding

Style : ● One's ○ Zero's

Spoofing

□ TCP KeepAlive

□ NetBIOS KeepAlive

☑ Enable RIP

Interface Cost

○ Unreachable

● 1

RIP Version

○ 1

○ 2

● Compatible

☑ Include default routes in RIP packets

☑ Ignore Incoming RIP Updates

4 Ensure that the Enable Broadcast Forwarding check box contains a check mark.

5 Select the broadcast style that matches the hosts on the Router's LAN (ones or zeros).

Note: When you select One's, the style is set for IP broadcasts over the LAN (for example, 89.255.255.255). Likewise, selecting Zero's sets the style to 89.0.0.0.

The broadcast style is most often One's and you should normally select this option.

6 Click OK.

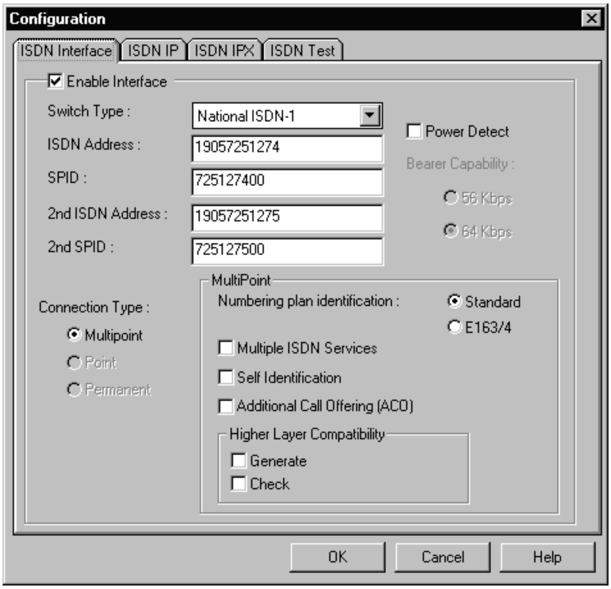
Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

To enable Broadcast Forwarding on the ISDN interface

1 Click the ISDN icon.

2 Select Properties from the pop-up menu that appears.

Result: The Configuration screen appears.



☑ Enable Interface

Switch Type : National ISDN-1

ISDN Address : 19057251274

SPID : 725127400

2nd ISDN Address : 19057251275

2nd SPID : 725127500

☐ Power Detect

Bearer Capability : ○ 56 Kbps ● 64 Kbps

Connection Type : ● Multipoint ○ Point ○ Permanent

MultiPoint

Numbering plan identification : ● Standard ○ E163/4

☐ Multiple ISDN Services

☐ Self Identification

☐ Additional Call Offering (ACO)

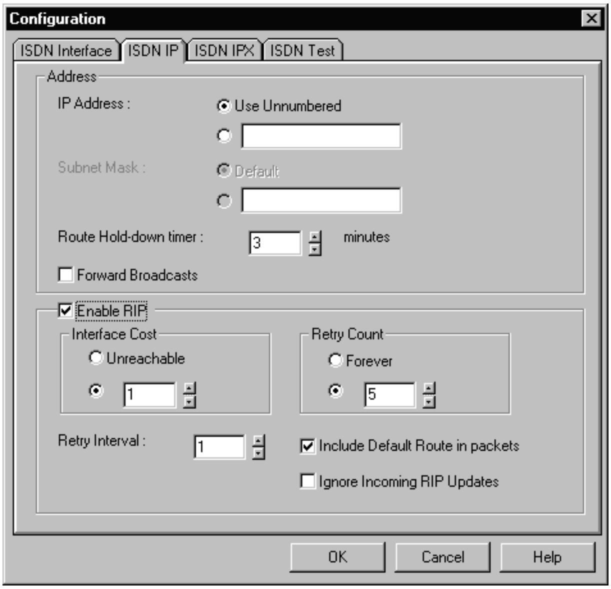
Higher Layer Compatibility

☐ Generate

☐ Check

3 Click the ISDN IP tab.

Result: The ISDN IP tab appears.



Address

IP Address : ● Use Unnumbered ○

Subnet Mask : ● Default ○

Route Hold-down timer : 3 minutes

□ Forward Broadcasts

☑ Enable RIP

Interface Cost ○ Unreachable ● 1

Retry Count ○ Forever ● 5

Retry Interval : 1

☑ Include Default Route in packets

□ Ignore Incoming RIP Updates

4 If you want to forward broadcasts onto the LAN, ensure that the Forward Broadcasts check box contains a check mark.

5 Click OK.

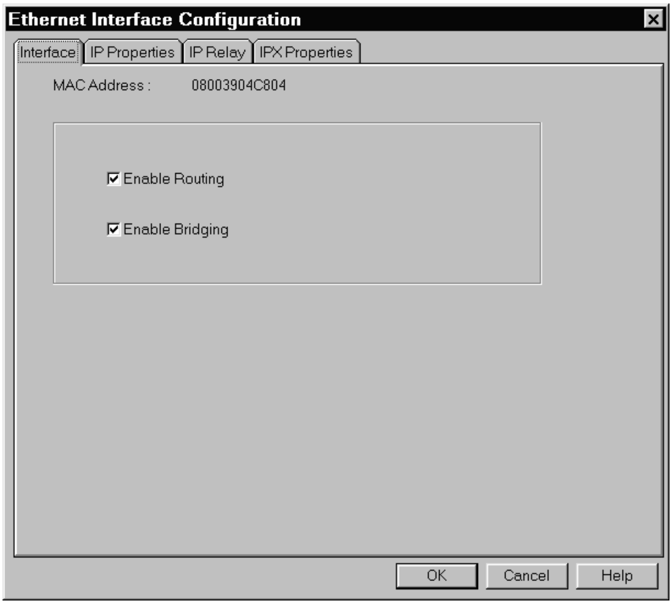
Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

To configure IP Relay table

1 Click the Ethernet icon.

2 Select Properties from the pop-up menu that appears.

Result: The Ethernet Interface Configuration screen appears.



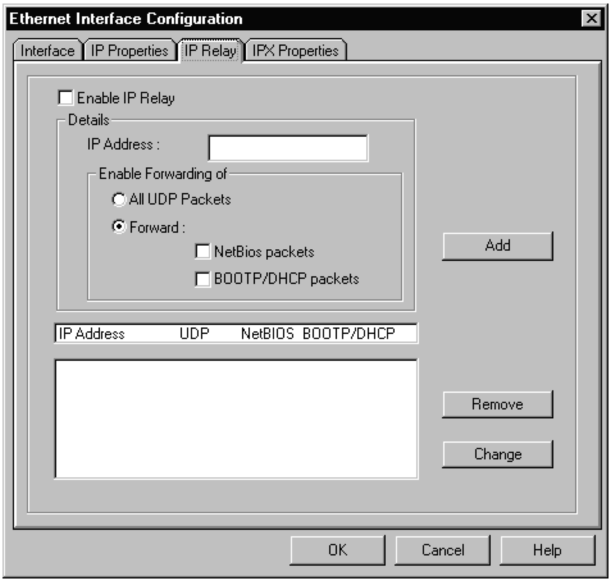
MAC Address : 08003904C804

☑ Enable Routing

☑ Enable Bridging

3 Click the IP Relay tab.

Result: The IP Relay tab appears.



☐ Enable IP Relay

Details

IP Address :

Enable Forwarding of

○ All UDP Packets

● Forward :

☐ NetBios packets

☐ BOOTP/DHCP packets

IP Address	UDP	NetBIOS	BOOTP/DHCP

4 Complete the fields as described in “IP Relay table field descriptions” below.

5 Click Add.

Result: The entry appears in the table at the bottom of the screen.

6 When you have entered all of the broadcast relays that you need, click OK.

Result: You return to the Configuration tab.

IP Relay table field descriptions

Field	Description
Enable IP Relay	Select this option if you want to use the IP addresses of NetBIOS or BootP devices.
IP Address	Enter one of the following: • the IP address of the NetBIOS or BootP/DHCP server that you want to receive broadcasts • the broadcast address of the network on which the server is located If there are several servers on one network, use the broadcast address. You can add up to 16 addresses to the table.
Enable Forwarding of All UDP Packets	Select this option if you want to forward all of the types of UDP broadcasts (including NetBIOS and BootP/DHCP broadcasts). If you want to forward only NetBIOS or BootP/DHCP packets, do not select this option. **Note:** If you forward all of the UDP broadcasts, you can keep your ISDN links open unnecessarily.

Field	Description
Forward	Select this option if you want to forward NetBIOS or BootP/DHCP packets, or both.
NetBios packets	Select this option if you want to forward NetBIOS packets.
BOOTP/DHCP packets	Select this option if you want to forward BootP/DHCP packets.

Spoofing

Introduction

Spoofing is the process that the HomeOffice Router uses to prevent meaningless traffic from keeping the network connection open. The Ethernet interface settings control some kinds of IP spoofing that the HomeOffice Router performs. This lets you determine, for some kinds of network traffic, whether the packets are meaningful.

Configuration overview

Note: Review this section completely before beginning any configuration.

Enable or disable TCP KeepAlive packets or NetBIOS KeepAlive packets, or both, on the Ethernet interface.

How it works

When you open a connection to a remote network, your computer and other devices on the local and remote networks send a constant stream of network traffic that can keep the network connection open, even when you are not using it for a specific purpose.

It can be expensive to keep the network connection open, so the HomeOffice Router closes the connection during idle periods, which are defined as times when no meaningful network traffic is flowing between the local and remote network.

The spoofing configuration defines the type of traffic that *should not* be sent (therefore, making the traffic meaningless).

What you can spoof

You can specify whether to spoof the following kinds of network packets:

- TCP KeepAlive packets

  Some older software sends these packets to keep the TCP connection active during idle periods. Since the HomeOffice Router can open and close the connection as needed, these packets are unnecessary and can be spoofed.

- NetBIOS KeepAlive packets

  Some software sends these packets to keep NetBIOS networking active during idle periods. These packets are unnecessary and can be spoofed.

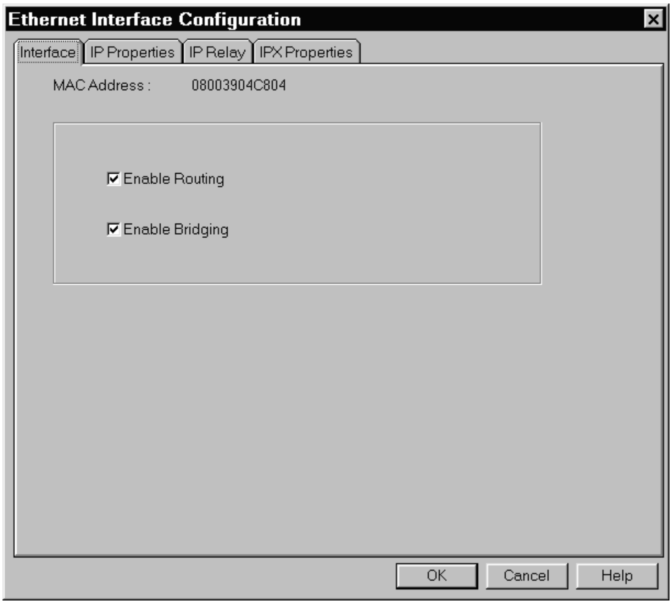
When to use spoofing

Use spoofing if you want to reduce ISDN line usage costs.

To enable spoofing

1. Click the Ethernet icon.
2. Select Properties from the pop-up menu that appears.

   Result: The Ethernet Interface Configuration screen appears.



Ethernet Interface Configuration

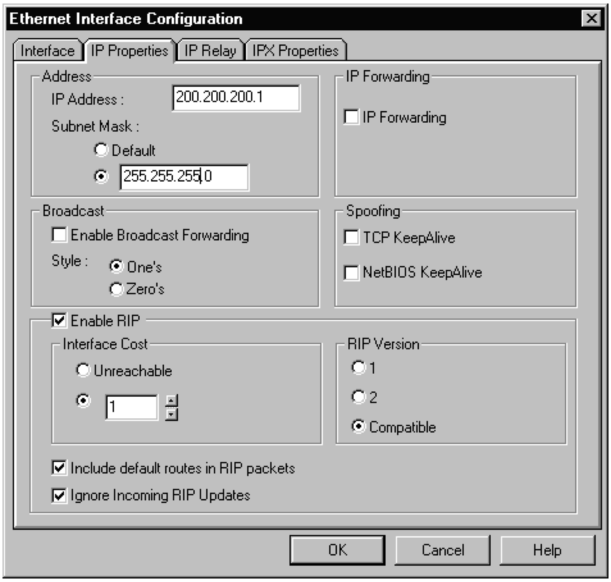
MAC Address : 08003904C804

☑ Enable Routing

☑ Enable Bridging

3 Click the IP Properties tab.

Result: The IP Properties tab appears.



Ethernet Interface Configuration

Address

IP Address : 200.200.200.1

Subnet Mask :

○ Default

● 255.255.255.0

IP Forwarding

□ IP Forwarding

Broadcast

□ Enable Broadcast Forwarding

Style : ● One's ○ Zero's

Spoofing

□ TCP KeepAlive

□ NetBIOS KeepAlive

☑ Enable RIP

Interface Cost

○ Unreachable

● 1

RIP Version

○ 1

○ 2

● Compatible

☑ Include default routes in RIP packets

☑ Ignore Incoming RIP Updates

4 In the Spoofing area, click the TCP KeepAlive check box to prevent these packets from being sent across the link when not necessary.

If you want all of the TCP KeepAlive packets to be sent between the local and remote networks, leave this check box blank.

5 Click the NetBIOS KeepAlive check box to prevent these packets from being sent across the link when not necessary.

If you want all of the NetBIOS KeepAlive packets to be sent between the local and remote networks, leave this check box blank.

6 Click OK.

Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

Bridging

Introduction

Bridging offers one of the most straightforward and flexible methods of interconnecting network segments. Bridges are very simple to use. Existing applications or communications software need no changes when bridges are introduced to a network.

If you set up the Router as a bridge/router, then IP is routed across the interfaces that have the IP protocol enabled, while all other protocols (DECnet, AppleTalk, Banyan Vines, SNA, and so on) are bridged.

Configuration overview

Note: Review this section completely before beginning any configuration.

You must give the Router an IP address only if you want to manage it from a network management station.

⚠ **CAUTION**

Risk of connection loss
If you want to use the Router for bridging only and you are attempting to configure it over the network, ensure that you enter a bridging IP address in the Bridging IP tab before you disable routing; otherwise, your connection to the Router will be lost.

1 Enable Bridging on the Ethernet interface (see page 270).

2 Configure a bridge (see page 271).

Benefits

With most bridges, you must only connect them to your network and turn them on. A bridge

- automatically learns the addresses of all active stations on its LAN
- examines all the packets on the LAN, reading their source and destination addresses
- forwards packets destined for a remote network to that network, over the WAN
- ignores or filters packets running between addresses on the local network

This means that traffic intended only for the local segment does not cross the bridge and clutter up the rest of the network.

Drawbacks and workaround

The bridge must forward some packets, such as broadcasts, multicasts, and packets with unknown destinations, across the WAN to all parts of the network. This can cause the following problems when bridging across ISDN:

- If you have configured more circuits than you have B-channels, the bridge tries to transmit broadcast and multicast packets, and packets with unknown destinations on all circuits. However, transmission must be complete on the first two circuits before more circuits can be opened. As a result, transmission is delayed on some circuits, or packets are discarded.
- Every broadcast and multicast transmission, or transmission to an unknown destination results in an ISDN call. Every call costs money.

The solution to both of these problems is to set up filtering to control the amount of traffic sent across ISDN links.

Filtering

Filtering tests whether a packet must be passed onto another network segment. It is designed to decrease the level of traffic on your network and is cost-effective because it eliminates most unnecessary traffic between networks.

You can set up filters based on the destination and source addresses of packets, access groups, packet type, and data content of packets. This helps to reduce the level of traffic passing over the ISDN link or prevents certain users from accessing the ISDN link.

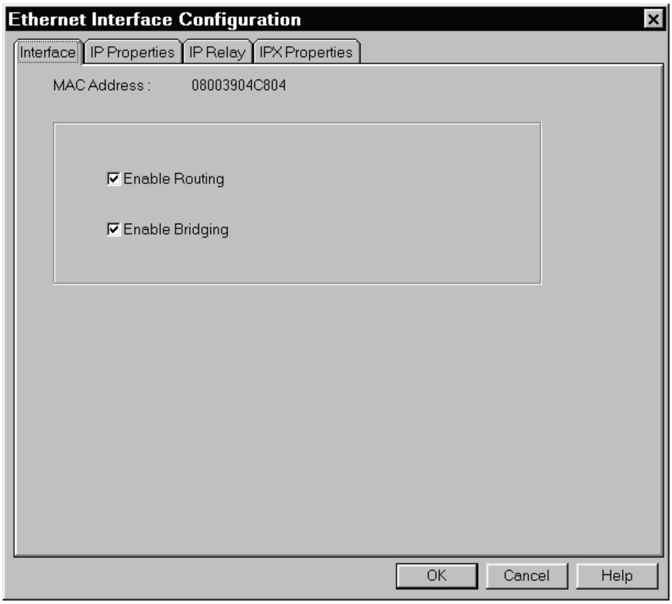
To configure the Router for bridge filtering, use the `bridge filter` command in the HomeOffice Router command shell. For instructions, refer to the *Meridian HomeOffice II Command Shell User Guide* (NTP 555-8321-910) on the Meridian HomeOffice II CD-ROM.

To enable Bridging on the Ethernet interface

1 Click the Ethernet icon.

2 Select Properties from the pop-up menu that appears.

Result: The Ethernet Interface Configuration screen appears.



Ethernet Interface Configuration

MAC Address : 08003904C804

☑ Enable Routing

☑ Enable Bridging

3 Ensure that the Enable Bridging check box is checked.

4 Click OK.

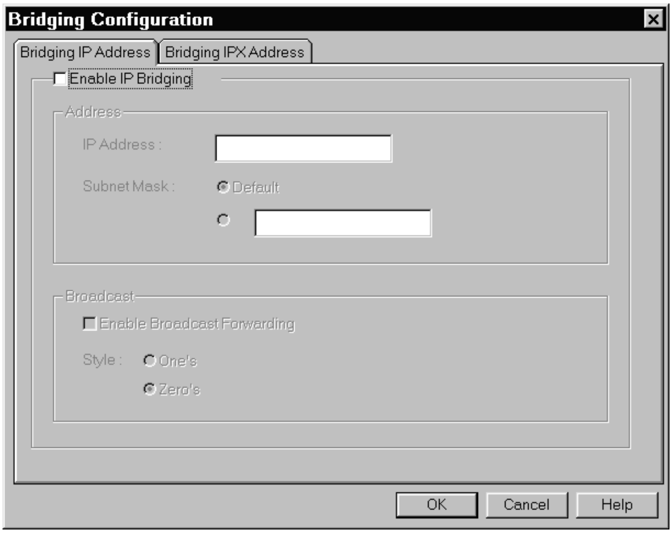
Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

To configure a bridge

1 Click the Admin icon.

2 Select Bridging from the pop-up menu that appears.

Result: The Bridging Configuration screen appears.



3 Complete the fields as described in “Bridging IP Address field descriptions” on page 272.

4 Click OK.

Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

Bridging IP Address field descriptions

Field	Description
Enable IP Bridging	Select this option if you want to activate the IP protocol for bridging interfaces.
IP Address	Enter the address of the interface that will be used for bridging. The address that you enter must be unique, and should conform to the addressing scheme used on your own network. **Caution:** You must enter a bridging IP address if you want to use your Router for bridging only and you are attempting to configure the Router over the network. If you select Bridging only on the Ethernet Interface tab without entering an IP address here first, you will lose your connection to the Router. The changed IP address takes effect only after you restart the Router.
Subnet Mask	Select this option if your network is simple. If your network requires subnetting, enter a subnet mask instead.
Enable Broadcast Forwarding	Select this option if you want broadcasts forwarded onto the LAN.
Style	Select the broadcast style that matches the hosts on your LAN: • Select One’s to set the style for IP broadcasts over the LAN to, for example, 89.255.255.255. • Select Zero’s to set the style to 89.0.0.0. The broadcast style is most often One’s and you should normally select this option.

Section E: Configuring the IPX network

In this section

Overview

Introduction

This section describes IPX/SPX features, when and why they should be used, and how to configure them.

Novell servers and workstations

This manual does not provide detailed instructions for configuring Novell servers and workstations. It only provides suggestions for what you must consider to keep ISDN usage costs down.

Refer to your Novell system documentation for configuration details.

IPX addresses

The Ethernet (MAC) address is the physical address of the HomeOffice Router on the LAN and should be 12 hexadecimal digits. It cannot be configured and is displayed for your information only.

An IPX node address identifies the address of the HomeOffice Router on the ISDN and Ethernet networks. An IPX node address is 12 hexadecimal digits in length.

The IPX network address identifies the network to which the HomeOffice Router is attached. The IPX network address must be 8 hexadecimal digits in length.

IPX Routing

Routing is the process of selecting the path for a packet being forwarded to another network device. Routes identify the destination IPX network, next network, next hop, and the number of ticks and hops used to reach the destination.

Routing should be the first option configured to maximize Router features such as DIAT and demand mode circuits. Routing minimizes the period in which the ISDN line is active.

RIP

Routing Information Protocol (RIP) is the dynamic routing protocol used on networks. The HomeOffice Router uses RIP over IPX to exchange routing information with other routers and to update the information in its routing table.

RIP is available on both the Ethernet and ISDN interfaces.

IPX Services and SAP

Service Advertising Protocol (SAP) is a protocol used by Novell Netware devices (such as printers, file servers, and gateways) to advertise their availability on the network by broadcasting their names, addresses, and current state. The HomeOffice Router uses SAP to exchange service information with other routers and to update the information in its services table.

SAP is available on both the Ethernet and the ISDN interface.

Filtering

SAP filtering allows you to specify the IPX services that are not broadcasted to other network devices. You can apply filtering on either incoming or outgoing services on the Ethernet or ISDN interface.

DIAT for IPX

Dynamic IPX Address Translation (DIAT for IPX) is a mechanism by which a remote network of one or more devices can appear as a single device to the host network. This allows the remote network the flexibility to implement an addressing scheme that is invisible to the host network.

Broadcast Forwarding

A broadcast is a network transaction that sends data to one or more hosts connected to the network.

You can forward the following types of networking packets to the remote network:

- broadcast
- NetBIOS
- NetWare security packets

Spoofing

Spoofing is the process by which the HomeOffice Router prevents meaningless traffic from keeping the network connection open. The Ethernet interface settings control some kinds of IPX spoofing that the HomeOffice Router performs. This lets you determine, for some kinds of network traffic, whether the packets are meaningful.

Bridging

Bridging offers one of the most straightforward and flexible methods of interconnecting network segments. Bridges are very simple to use. Existing applications or communications software need no changes when bridges are introduced to a network.

If you set up your device as a bridge/router, then IPX is routed across the interfaces that have the IPX protocol enabled, while all other protocols (DECnet, AppleTalk, Banyan Vines, SNA, and so on) are bridged.

Novell server and workstation setup

Introduction

You can find exact details of how to set up your Novell servers and workstations in your Novell system documentation. These details vary from system to system.

Things to consider

Note the following:

- Ensure that all the devices on a network have the same network address, including routers, servers, and workstations.
- When using Novell servers that have internal network addresses, the HomeOffice Router needs routes defined to the internal network address of the server, as well as to any physical network.
- Ensure that you set the correct data link type for your Ethernet.
- Consider the way in which ISDN is provisioned, particularly if you are using Novell 4.0 or later.

You should define the appropriate spoofing type for your network to keep network costs down.

Optimizing server parameters with NetWare V4.1

If you are running NetWare version 4.1 and have servers that are connected over ISDN, then you can set some server parameters to minimize ISDN usage.

Change the following parameters from their default values:

- set timesync polling interval = 86400 (that is, set it to 24 hours; the default is 10 minutes)
- set nds synchronization interval = 1440 (that is, set it to 24 hours; the default is 30 minutes)

Refer to your NetWare documentation for information on how to set these parameters (for example, look for `servman` in the index).

Note: When using NetWare V4.1, it is important to monitor your ISDN usage. Consult a Novell support engineer for further details.

IPX address, network number, and node number

Introduction

This section explains what the MAC, node, and network addresses are and how to configure them. You must assign an IPX address to every device on the network.

Ethernet MAC address

The Ethernet (MAC) address is the physical address of the HomeOffice Router on the LAN and should be 12 hexadecimal digits. It cannot be configured and is displayed for your information only.

080039123456 is an example of a MAC address.

IPX node address

An IPX node address identifies the address of the HomeOffice Router on the ISDN and Ethernet networks. An IPX node address is 12 hexadecimal digits in length.

On the Ethernet interface, the HomeOffice Router automatically uses its physical (MAC) address as its node address and, therefore, does not need to be configured (or shown) on the Ethernet interface.

On the ISDN interface, the IPX node address must be configured (and is shown). When configuring with the Install Wizard, the HomeOffice Router’s MAC address is used by default.

IPX network address

The IPX network address identifies the network to which the HomeOffice Router is attached.

The IPX network address must be 8 hexadecimal digits in length. On the Ethernet network, the IPX network address should be the same as the network number of any IPX servers on the Ethernet network.

Network ticks

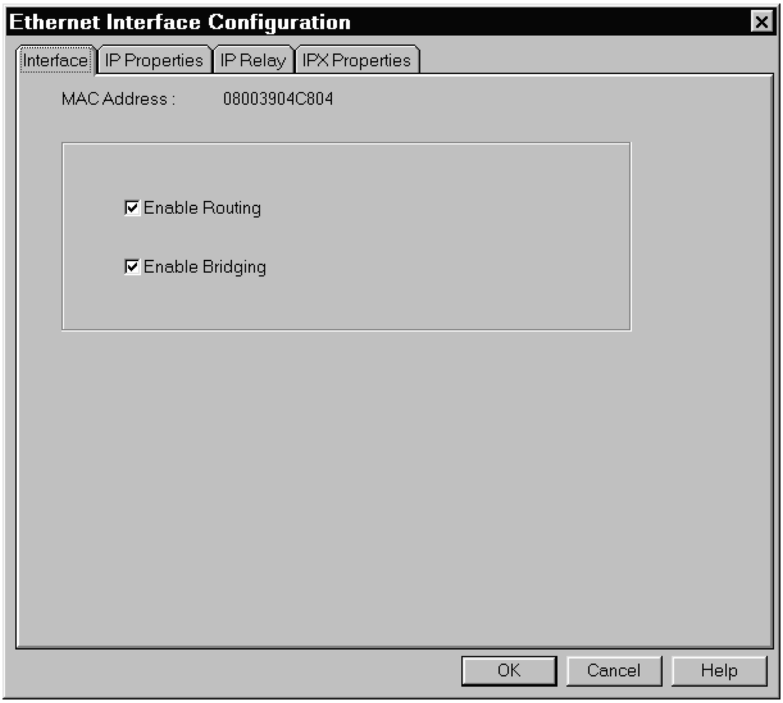
The number of ticks is a measure of the time required to deliver a 576-byte packet to a node on the network specified on the Ethernet and ISDN interfaces. Each tick represents 1/18ths of a second.

For wide area links, the time depends upon the line speed and how busy the line is. Values should be conservative (that is, long) and never shorter than 2 seconds (36 ticks). The shortest (fastest) value that you should set for ISDN is 5/18ths second (5 or 6 ticks).

To view the HomeOffice Router's MAC address

1. Click the Ethernet icon.
2. Select Properties from the pop-up menu that appears.

   Result: The Ethernet Interface Configuration screen appears.



MAC Address : 08003904C804

☑ Enable Routing

☑ Enable Bridging

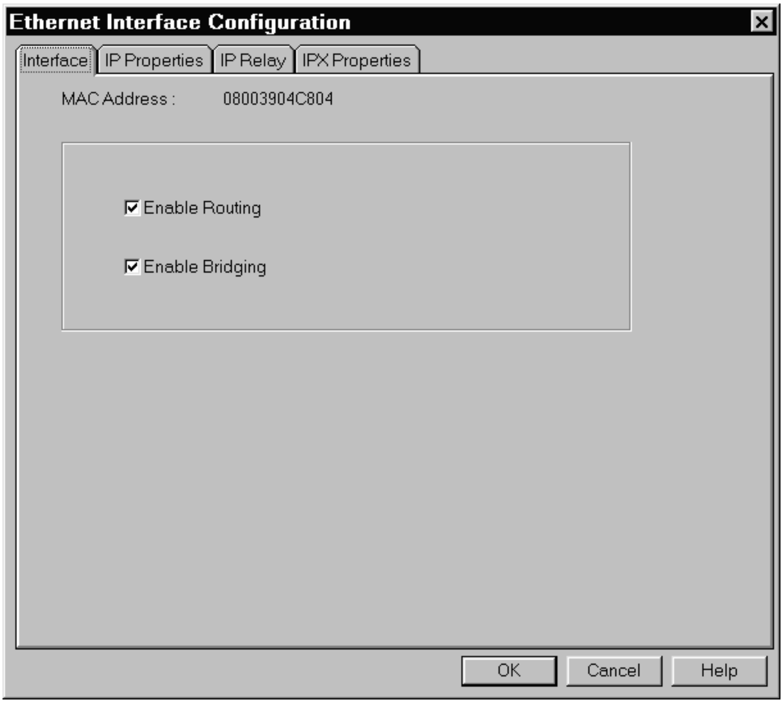
3 Review the MAC Address field.

To configure the IPX network address on the Ethernet interface

1 Click the Ethernet icon.

2 Select Properties from the pop-up menu that appears.

Result: The Ethernet Interface Configuration screen appears.



Ethernet Interface Configuration

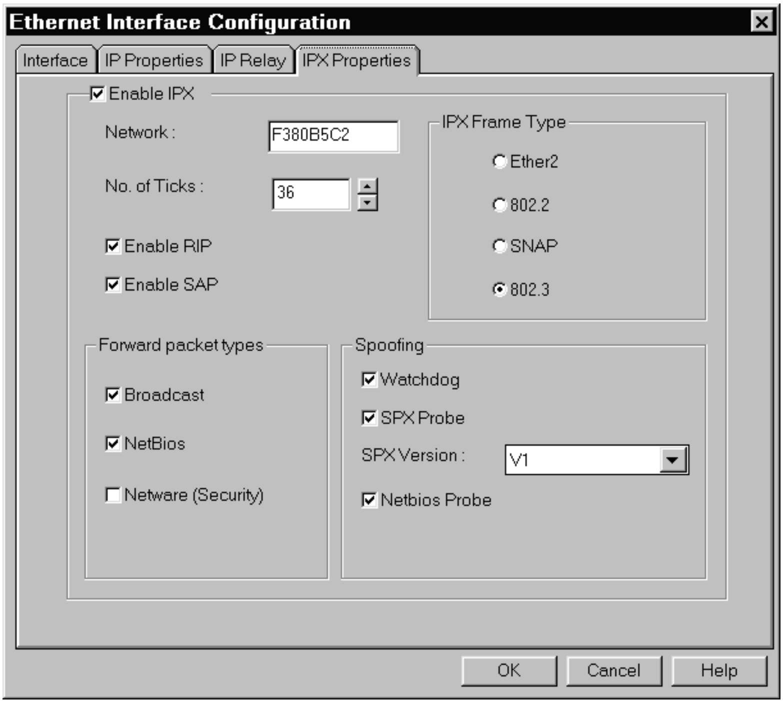
MAC Address : 08003904C804

☑ Enable Routing

☑ Enable Bridging

3 Click the IPX Properties tab.

Result: The IPX Properties tab appears.



☑ Enable IPX

Network : F380B5C2

No. of Ticks : 36

☑ Enable RIP

☑ Enable SAP

IPX Frame Type

○ Ether2

○ 802.2

○ SNAP

● 802.3

Forward packet types

☑ Broadcast

☑ NetBios

□ Netware (Security)

Spoofing

☑ Watchdog

☑ SPX Probe

SPX Version : V1

☑ Netbios Probe

4 Ensure that Enable IPX is checked.

5 Enter the IPX address into the Network field.

6 Accept the default for the number of ticks. (The default is 36.)

7 Click OK.

Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

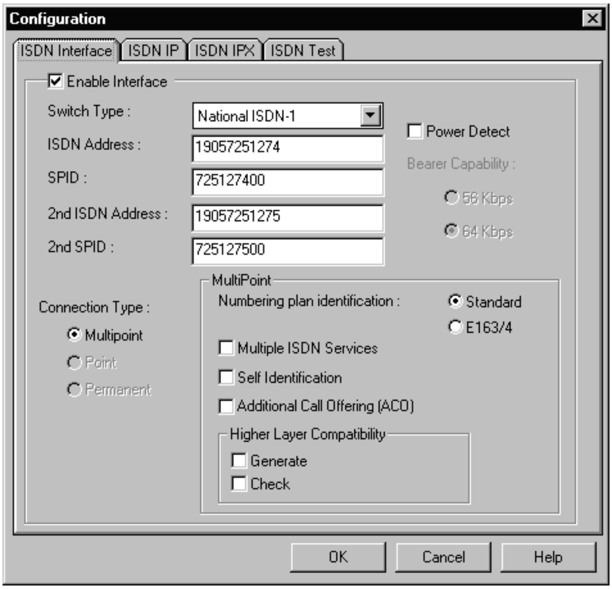
Note: If you do not configure a valid IP address on the IP Properties tab, then you are prompted to enter that first before the HomeOffice Router reconfigures with the IPX network address.

To configure the IPX node and network addresses on the ISDN interface

1 Click the ISDN icon.

2 Select Properties from the pop-up menu that appears.

Result: The Configuration screen appears.



☑ Enable Interface

Switch Type : National ISDN-1

ISDN Address : 19057251274

SPID : 725127400

2nd ISDN Address : 19057251275

2nd SPID : 725127500

□ Power Detect

Bearer Capability : ○ 56 Kbps ● 64 Kbps

Connection Type : ● Multipoint ○ Point ○ Permanent

MultiPoint

Numbering plan identification : ● Standard ○ E163/4

□ Multiple ISDN Services

□ Self Identification

□ Additional Call Offering (ACO)

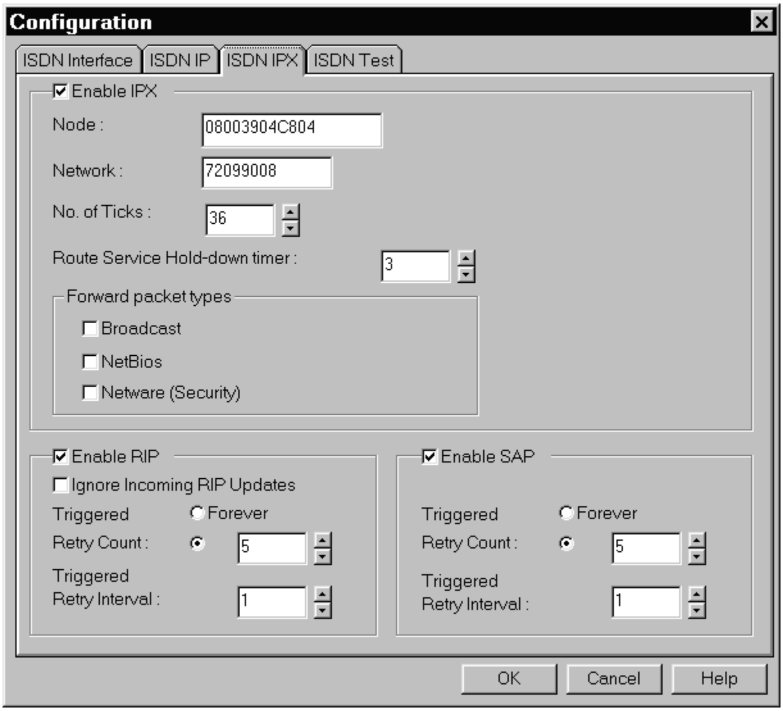
Higher Layer Compatibility

□ Generate

□ Check

3 Click the ISDN IPX tab.

Result: The ISDN IPX tab appears.



☑ Enable IPX

Node : 08003904C804

Network : 72099008

No. of Ticks : 36

Route Service Hold-down timer : 3

Forward packet types

□ Broadcast

□ NetBios

□ Netware (Security)

☑ Enable RIP

□ Ignore Incoming RIP Updates

Triggered Retry Count : ○ Forever ● 5

Triggered Retry Interval : 1

☑ Enable SAP

Triggered Retry Count : ○ Forever ● 5

Triggered Retry Interval : 1

4 Ensure that Enable IPX is checked.

5 Enter the node address.

Note: The node address must be 12 hexadecimal digits in length.

6 Enter the network address.

Note: The network address must be 8 hexadecimal digits in length.

7 Accept the default for the number of ticks. (The default is 36.)

8 Enter the number of ticks between 1 and 65535.

9 Click OK.

Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

IPX Routing

Introduction

Routing is the process of selecting the path for a packet that is being forwarded to another network device. Routes identify the destination IPX network, next network, next hop, and the number of ticks and hops used to reach the destination.

Configuration overview

Note: Review this section completely before beginning any configuration.

To configure Routing for the Ethernet interface

1. Enable Routing on the Ethernet interface (see page 290).
2. Enter static routes into the IPX Routes table (see page 295).

To configure Routing for the ISDN interface

1. Enable Routing on an ISDN circuit (see page 291).
2. Configure the network address and route service hold-down timer on the ISDN interface (see page 292).
3. Enter static routes into the IPX Routes table (see page 295).

When to use Routing

You should configure routing as the first option to maximize Router features such as DIAT and demand mode circuits. Routing minimizes the period in which the ISDN line is active.

Types of routing

Static routing

Routes that are defined in a routing table are static routes. To select a suitable route, the Router first identifies the network to which the packets are being sent, and then selects a route with a matching destination network address.

If you choose static routing for the connection, a route is generally defined to the host network. In most telecommuter configurations, a default route to the next hop remote access switch is sufficient. This default route is defined on the HomeOffice Router when you use the Install Wizard to configure a circuit. If you require additional routes (to other telecommuter units, for example), then you must consider routing table capacity and administrative requirements.

Dynamic routing

If your host computers understand Routing Information Protocol (RIP), then you can use RIP on both the ISDN and Ethernet interfaces of the HomeOffice Router. RIP automatically updates each host's routing table.

If you want to use dynamic routing, see "Routing Information Protocol" on page 298 for more information.

Benefits and drawbacks of using Routing

Benefits

Routing

- provides an efficient method of managing network traffic
- reduces the effect of network broadcast packets
- enables network interface devices to maintain updated routing information

Drawbacks

Routing

- requires additional consideration in network planning details
- does not inherently pass all of the types of protocols without additional provisioning
- requires additional administration

When to use the routing table

If a telecommuter connects only to a central site on the corporate network, then you require a default route to the remote access switch interface. When configuring the telecommuter’s circuit with the Install Wizard, a default circuit is created and subsequently is the only route configured in the IPX Routing table. A routing table is required, even if it contains only one route (the default route).

You can configure up to 34 static entries in the IPX Routing table. Statically entered routing addresses (stored permanently in the IPX Routing table) define the routes by which the HomeOffice Router reaches remote networks. You can enter up to three static routes to any remote network.

The routing table that you set up on each host might look like this:

Destination network	Next network	Next node
00000008	72099008	80039121134
00000007	72099008	3FB788A6D50C

Prerequisites for static routes over ISDN

Before adding ISDN routes to the IPX Routing table, ensure you do the following:

- Set up the ISDN interface using the ISDN Interface dialog box.

  For instructions, see “Configuring the ISDN interface” on page 107.
- Decide on the addressing information that you require.

  In this case, you require the IPX addresses of the remote devices and the ISDN addresses of the ISDN interfaces. You should also think of an appropriate name for the circuit.

How multiple static routes work

Multiple static routes are a cost-saving alternative to running RIP over WAN links.

The HomeOffice Router detects if the best route (as defined by the metric value) becomes unavailable, and uses the next best route. If the original best route returns to service, it replaces the alternative route. Since the Router determines which route to use, you do not need to run RIP over the ISDN link.

When a static route is detected as being down (that is, when the physical link breaks), it can take up to 3 minutes for an alternative route to be used. This is the length of time that it takes for RIP running on either side of the ISDN link to broadcast the routing topology change throughout the network. This is the way RIP normally works.

You may decide that static routes provide the network resilience that you require, while avoiding the possible expense of standard RIP, or the limitations of Triggered RIP.

Route service hold-down timer

The route service hold-down timer applies only to the ISDN interface.

When the Router realizes that an ISDN circuit is not responding, it deletes all of the routes dependent on that circuit. The route service hold-down timer is the number of minutes that should elapse between the Router realizing that a circuit has gone down and the deletion of all dependent routes.

A route hold-down timer of 3 minutes is recommended. A value of less than 3 minutes can be appropriate when a faster response to the failure of a circuit is required. This is recommended only if the device is operating on a leaf node of the network. Within a mesh, changing this timer can have unpredictable results if other RIP entities are running with the default timing.

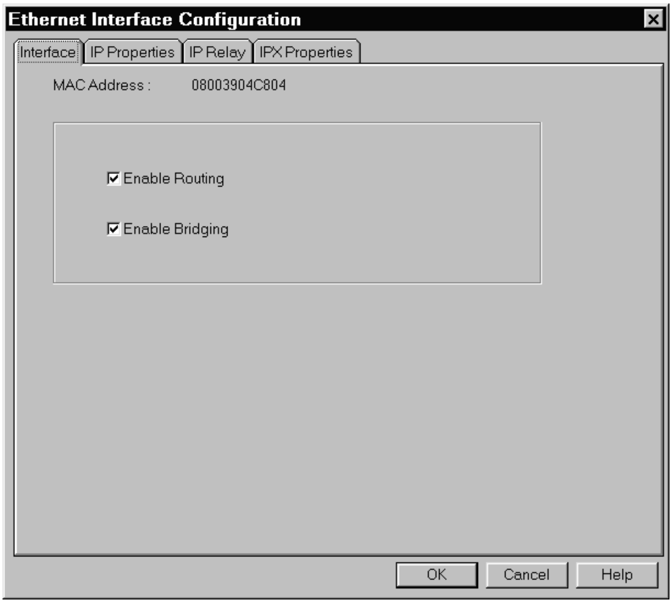
The default of 3 minutes is suitable for most situations. If you increase this timer, then it has the effect of reducing the number of network reconfigurations on networks that suffer short-term link failures or congestion. The network also takes longer to reconfigure when a permanent link failure occurs.

To enable Routing on the Ethernet interface

1 Click the Ethernet icon.

2 Select Properties from the pop-up menu that appears.

Result: The Ethernet Interface Configuration screen appears.



Ethernet Interface Configuration

MAC Address : 08003904C804

☑ Enable Routing

☑ Enable Bridging

3 Ensure that Enable Routing is selected.

4 Click OK.

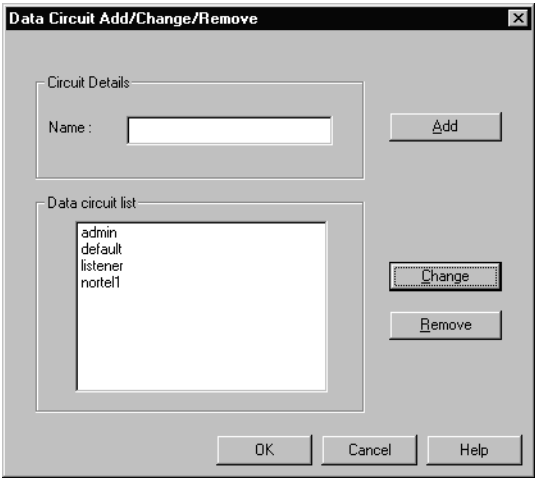
Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

To enable Routing on the ISDN circuit

1 Click the ISDN icon.

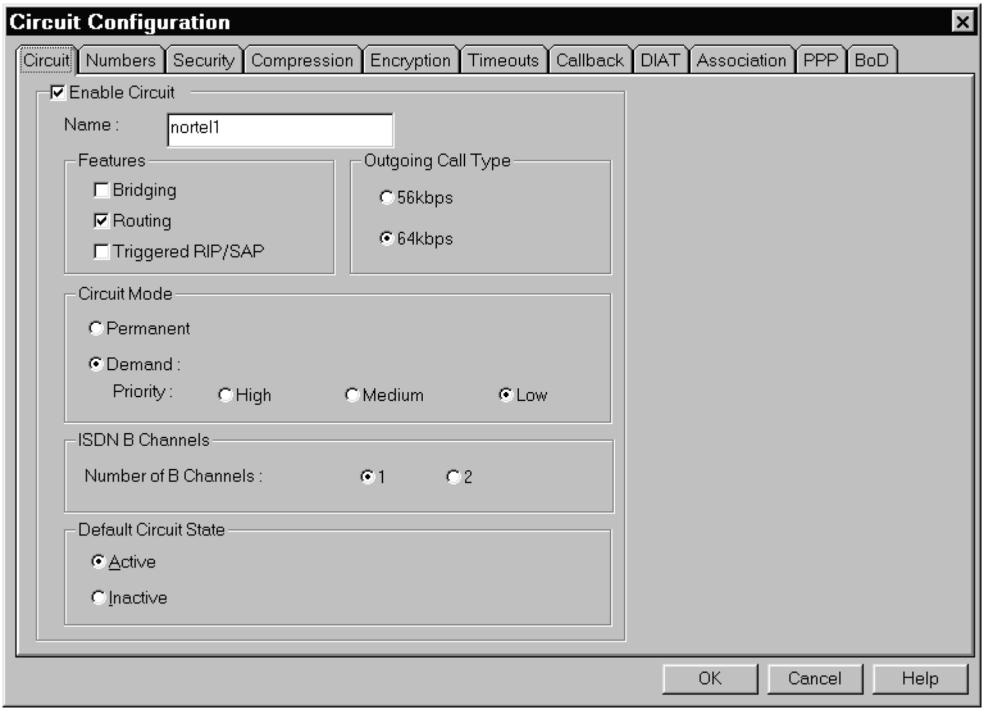
2 Select Circuits from the pop-up menu that appears.

Result: The Data Circuit Add/Change/Remove screen appears.



3 Select the circuit for which you want to enable Routing, and then click Change.

Result: The Circuit Configuration screen appears.



Circuit Configuration

☑ Enable Circuit

Name : nortel1

Features

- ☐ Bridging
- ☑ Routing
- ☐ Triggered RIP/SAP

Outgoing Call Type

- ○ 56kbps
- ● 64kbps

Circuit Mode

- ○ Permanent
- ● Demand :

Priority : ○ High ○ Medium ● Low

ISDN B Channels

Number of B Channels : ● 1 ○ 2

Default Circuit State

- ● Active
- ○ Inactive

4 On the Circuit tab, ensure that Routing is selected.

5 Click OK.

Result: The Data Circuit Add/Change/Remove screen appears.

6 Click OK again.

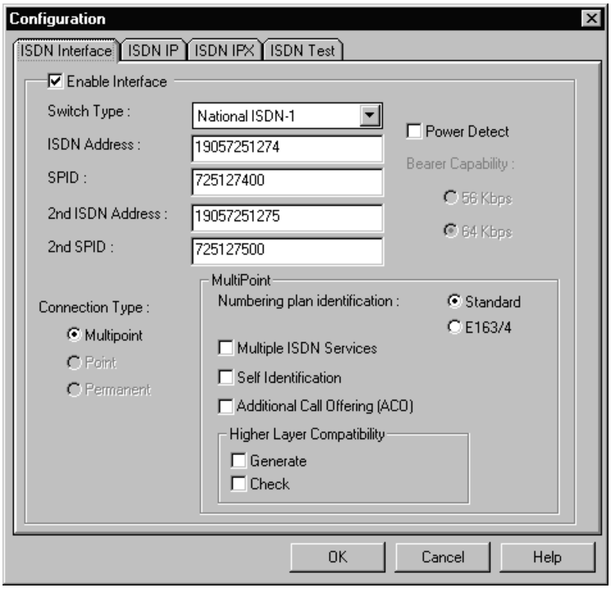
Result: You return to the Configuration tab.

To configure Routing on the ISDN interface

1 Click the ISDN icon.

2 Select Properties from the pop-up menu that appears.

Result: The Configuration screen appears.



☑ Enable Interface

Switch Type : National ISDN-1

ISDN Address : 19057251274

SPID : 725127400

2nd ISDN Address : 19057251275

2nd SPID : 725127500

□ Power Detect

Bearer Capability : ○ 56 Kbps ● 64 Kbps

Connection Type : ● Multipoint ○ Point ○ Permanent

MultiPoint

Numbering plan identification : ● Standard ○ E163/4

□ Multiple ISDN Services

□ Self Identification

□ Additional Call Offering (ACO)

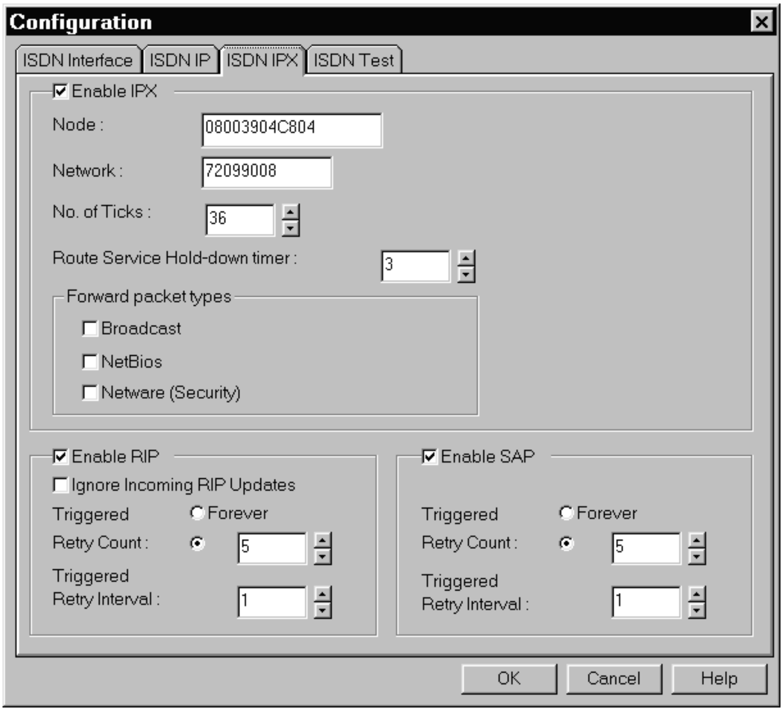
Higher Layer Compatibility

□ Generate

□ Check

3 Click the ISDN IPX tab.

Result: The ISDN IPX tab appears.


Configuration

☑ Enable IPX

Node : 08003904C804

Network : 72099008

No. of Ticks : 36

Route Service Hold-down timer : 3

Forward packet types

□ Broadcast

□ NetBios

□ Netware (Security)

☑ Enable RIP

□ Ignore Incoming RIP Updates

Triggered Retry Count : ○ Forever ● 5

Triggered Retry Interval : 1

☑ Enable SAP

Triggered Retry Count : ○ Forever ● 5

Triggered Retry Interval : 1

4 Ensure that the Network field contains the IPX address of the ISDN interface.

5 Accept the default for the Route Service Hold-down timer. (The default is 3.)

6 Click OK.

Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

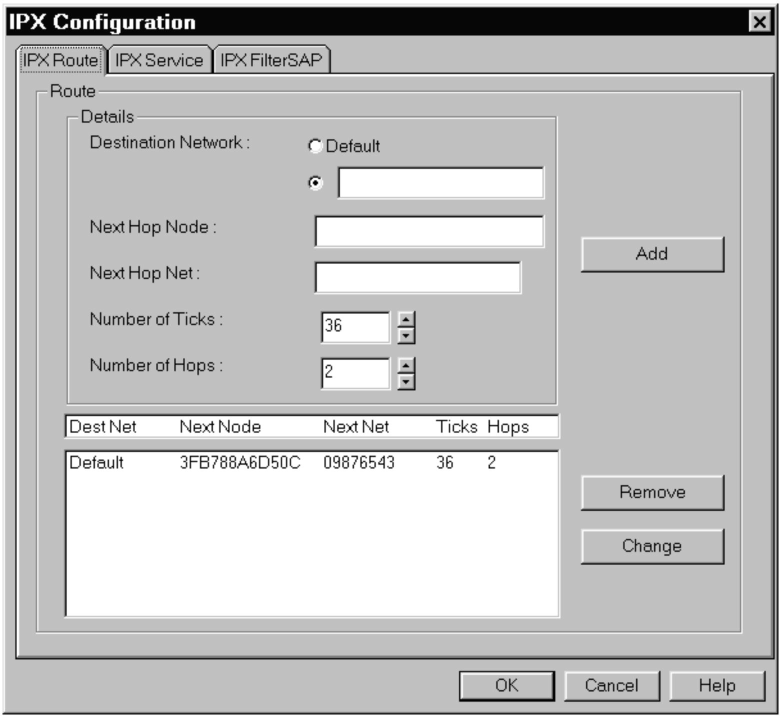
To create IPX routes

Note: If two routes have identical names, the Router uses the static route and ignores the dynamic route.

1 Click the Admin icon.

2 Select IPX Properties from the pop-up menu that appears.

Result: The IPX Configuration screen appears.



IPX Configuration

Route

Details

Destination Network : ○ Default ●

Next Hop Node :

Next Hop Net :

Number of Ticks : 36

Number of Hops : 2

Dest Net	Next Node	Next Net	Ticks	Hops
Default	3FB788A6D50C	09876543	36	2

3 Complete the fields as described in “Routing table field descriptions” on page 296.

4 Click Add.

Result: If all of the entries are valid, then the route is added to the table at the bottom of the screen. If one or more entries are invalid, then an error message appears.

5 Click OK.

Result: You return to the Configuration tab.

Routing table field descriptions

Field	Description
Destination Network	Click Default or enter the address of the final destination network. The IPX address must be in hexadecimal format and must not be a network to which the Router is directly connected. **Note:** You can add up to three routes to the same destination network.
Next Hop Node	Enter the node address of the next router down the line towards the destination network. The next hop node must be on a network to which the Router is directly connected. The IPX node address must be 12 hexadecimal digits in length.
Next Hop Net	Enter the network address of the next router down the line toward the destination network. The IPX network address must be 8 hexadecimal digits in length.
Number of Ticks	It is recommended that you accept the default of 36. If you choose to change the number of ticks, enter a number between 1 and 65535. 18 ticks equals 1 second. **Notes:** • If two routes have the same number of ticks, then the route with the smallest number of hops is used (that is, the route that involves the smallest number of routers). • You can enter an artificially high or low number of ticks and hops to force your Router to use (or not use) a particular route.

Field	Description
Number of Hops	Enter the number of hops (or routers) that it takes to reach the destination network. The number of hops is the number of routers that traffic must travel through to reach the destination. This number must be between 1 and 15. Packets are sent over the route with the lowest metric. **Note:** You can enter an artificially high or low metric to force the Router to use (or not use) a particular route. The default is 2.

Routing Information Protocol

Introduction

Routing Information Protocol (RIP) is the dynamic routing protocol used on networks. The HomeOffice Router uses RIP over IPX to exchange routing information with other routers and to update the information in its routing table.

RIP is available on both the Ethernet and ISDN interfaces. You may decide not to run RIP on the ISDN interface to reduce costs. However, you should keep RIP running on the Ethernet (LAN) interface, because this does not affect connection costs.

Configuration overview

Note: Review this section completely before beginning any configuration.

Ethernet interface

Enable RIP on the Ethernet interface (see page 301). RIP is enabled by default when configuring with the Install Wizard.

ISDN interface

1 Configure RIP on the ISDN interface (see page 227).

2 Configure RIP on an ISDN circuit (see page 229).

Types of RIP

Standard RIP

Normally, you use RIP on a network to pass messages to other routers. When RIP operates in the standard way, messages are sent every 60 seconds. These messages tell the other routers that the source router is active and viable. Standard RIP uses ISDN bandwidth and causes unnecessary calls on wide area networks. Standard RIP is not recommended for ISDN.

Instead of confirming availability at frequent intervals (Broadcast RIP), you can configure routing information statically in a routing table. The routing table is an adequate solution for less complex networks, but it is very time-consuming for the administrator.

Triggered RIP

Triggered RIP is a method of keeping costs down on ISDN WANs. Triggered RIP is beneficial for more complex networks where the configuration may change.

When you use Triggered RIP, the Router and other devices exchange RIP information when the Router is powered up. Instead of repeating this information, the Router and other devices do not exchange packets until the configuration changes. Configuration changes trigger update messages.

Triggered RIP gives you the benefit of dynamically updating routing information without using excessive bandwidth. Update messages are sent only when the router detects a change in its routing database. This means that routing data is sent only when required, reducing ISDN usage and costs, while still being responsive to topology changes.

Note: If you set the ISDN address to call to DISABLED on a circuit, then you must also disable support for Triggered RIP. You cannot make outgoing calls on that circuit.

When to use RIP

Use RIP when

- route selection must happen quickly to prevent network congestion (the use of routing tables can be time-consuming)
- you do not want to maintain routing tables

On the Ethernet interface

Use RIP on the Ethernet interface if the telecommuter has created subnets (with the use of additional routers and bridges) on his or her own network.

On the ISDN interface

Use RIP on the ISDN interface if the telecommuter’s LAN participates as an additional network (or series of subnets) recognized by the host network (DIAT is disabled). Under these circumstances, the HomeOffice Router receives regular updates on routing information by any other RIP router on the same WAN subnet.

Benefits

On the Ethernet interface

When you use RIP on the Ethernet interface

- the HomeOffice Router can exchange RIP updates with routers (if present) on the same subnet of the telecommuter’s LAN
- it is unnecessary to manually update the HomeOffice Router’s routing table

On the ISDN interface

When you use RIP on the ISDN interface

- the HomeOffice Router can exchange RIP updates with routers on the same WAN subnet of the host or central LAN
- it is unnecessary to manually update the HomeOffice Router’s routing table

Drawbacks

On the Ethernet interface

When you use RIP on the Ethernet interface, there is no significant reduction in performance, regardless of whether the telecommuter’s network consists of additional subnets.

On the ISDN interface

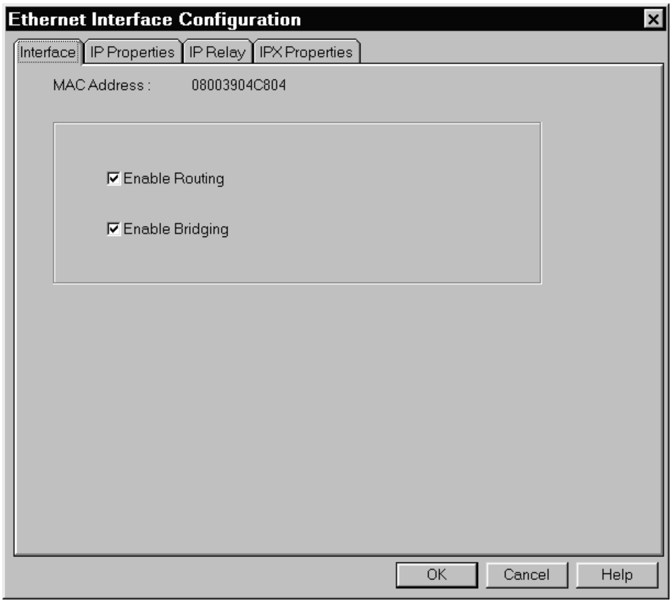
You should carefully consider RIP on the ISDN interface. The HomeOffice Router can be inundated with RIP broadcasts, which results in repeated costly activation of the ISDN circuit. If the HomeOffice Router requires only a single route to the remote access switch on the host network, a static entry for this route is recommended.

To enable RIP on the Ethernet interface

1 Click the Ethernet icon.

2 Select Properties from the pop-up menu that appears.

Result: The Ethernet Interface Configuration screen appears.



Ethernet Interface Configuration

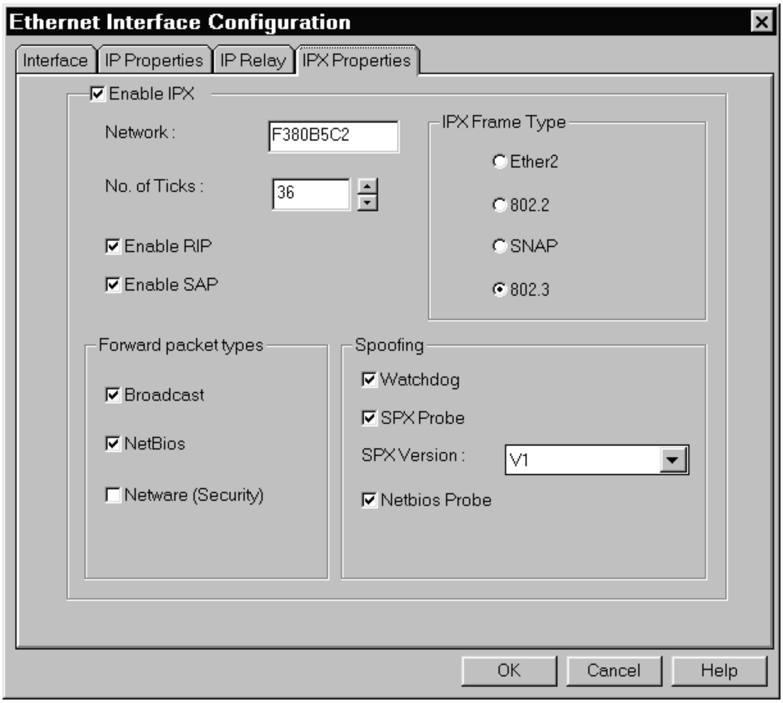
MAC Address : 08003904C804

☑ Enable Routing

☑ Enable Bridging

3 Click the IPX Properties tab.

Result: The IPX Properties tab appears.



☑ Enable IPX

Network : F380B5C2

No. of Ticks : 36

☑ Enable RIP

☑ Enable SAP

IPX Frame Type

○ Ether2

○ 802.2

○ SNAP

● 802.3

Forward packet types

☑ Broadcast

☑ NetBios

□ Netware (Security)

Spoofing

☑ Watchdog

☑ SPX Probe

SPX Version : V1

☑ Netbios Probe

4 Click Enable RIP.

5 Click OK.

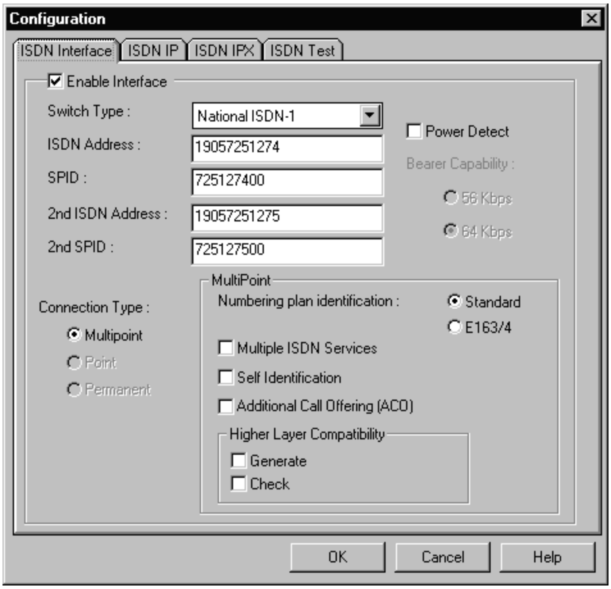
Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

To configure RIP on the ISDN interface

1 Click the ISDN icon.

2 Select Properties from the pop-up menu that appears.

Result: The Configuration screen appears.



☑ Enable Interface

Switch Type : National ISDN-1

ISDN Address : 19057251274

SPID : 725127400

2nd ISDN Address : 19057251275

2nd SPID : 725127500

□ Power Detect

Bearer Capability :

○ 56 Kbps

● 64 Kbps

Connection Type :

● Multipoint

○ Point

○ Permanent

MultiPoint

Numbering plan identification : ● Standard ○ E163/4

□ Multiple ISDN Services

□ Self Identification

□ Additional Call Offering (ACO)

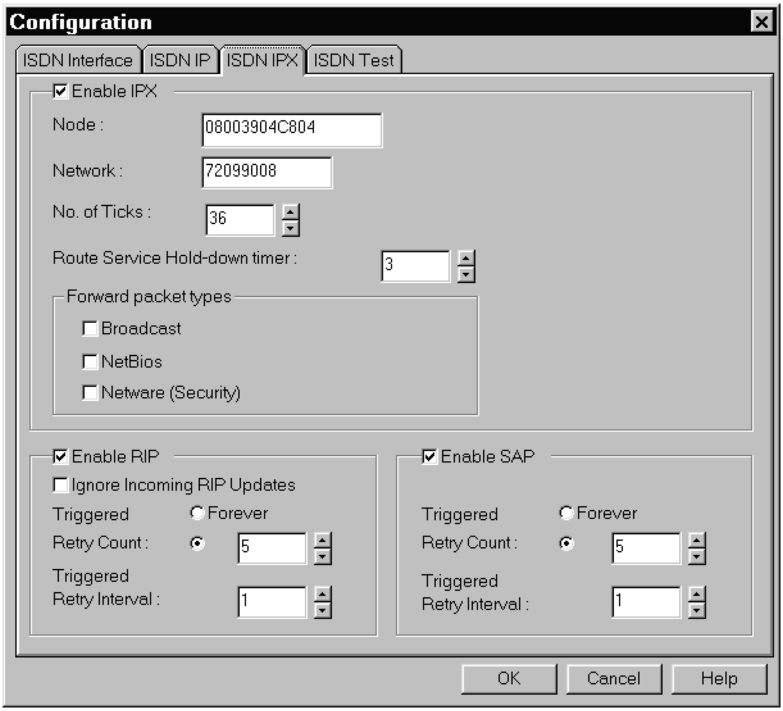
Higher Layer Compatibility

□ Generate

□ Check

3 Click the ISDN IPX tab.

Result: The ISDN IPX tab appears.



☑ Enable IPX

Node : 08003904C804

Network : 72099008

No. of Ticks : 36

Route Service Hold-down timer : 3

Forward packet types

□ Broadcast

□ NetBios

□ Netware (Security)

☑ Enable RIP

□ Ignore Incoming RIP Updates

Triggered Retry Count : ○ Forever ● 5

Triggered Retry Interval : 1

☑ Enable SAP

Triggered Retry Count : ○ Forever ● 5

Triggered Retry Interval : 1

4 Click Enable RIP.

5 Complete the fields as described in the “RIP field descriptions” on page 307.

6 Click OK.

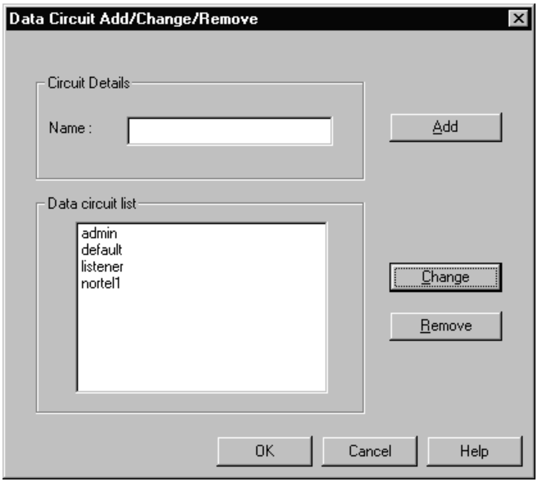
Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

To configure RIP on an ISDN circuit

1 Click the ISDN icon.

2 Select Circuits from the pop-up menu that appears.

Result: The Data Circuit Add/Change/Remove screen appears.



Data Circuit Add/Change/Remove

Circuit Details

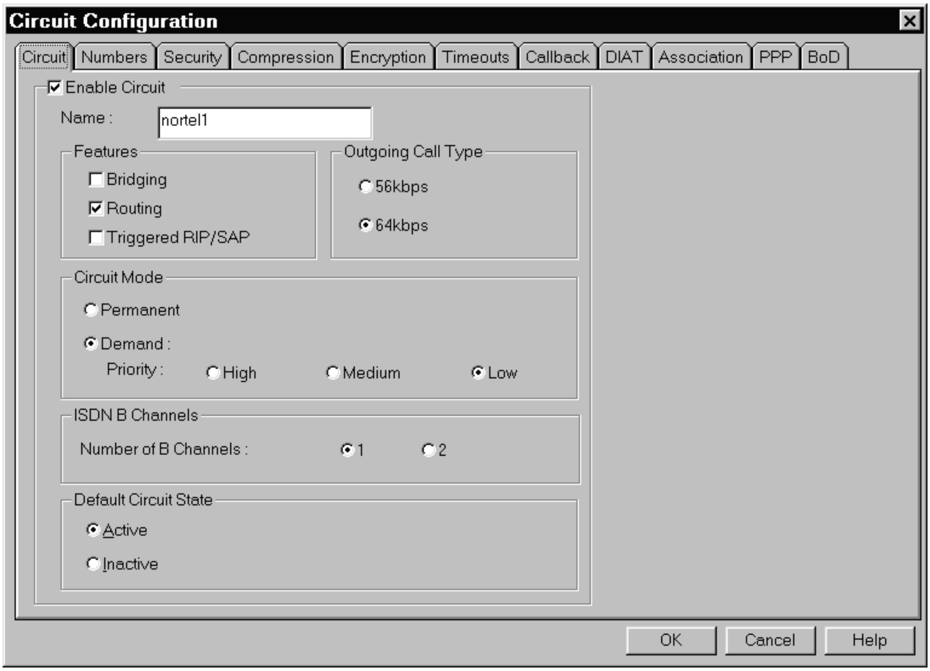
Name :

Data circuit list

admin
default
listener
nortel1

3 Select the circuit for which you want to configure RIP, and then click Change.

Result: The Circuit Configuration screen appears.



Circuit Configuration

☑ Enable Circuit

Name : nortel1

Features

☐ Bridging
☑ Routing
☐ Triggered RIP/SAP

Outgoing Call Type

○ 56kbps
● 64kbps

Circuit Mode

○ Permanent
● Demand :
Priority : ○ High ○ Medium ● Low

ISDN B Channels

Number of B Channels : ● 1 ○ 2

Default Circuit State

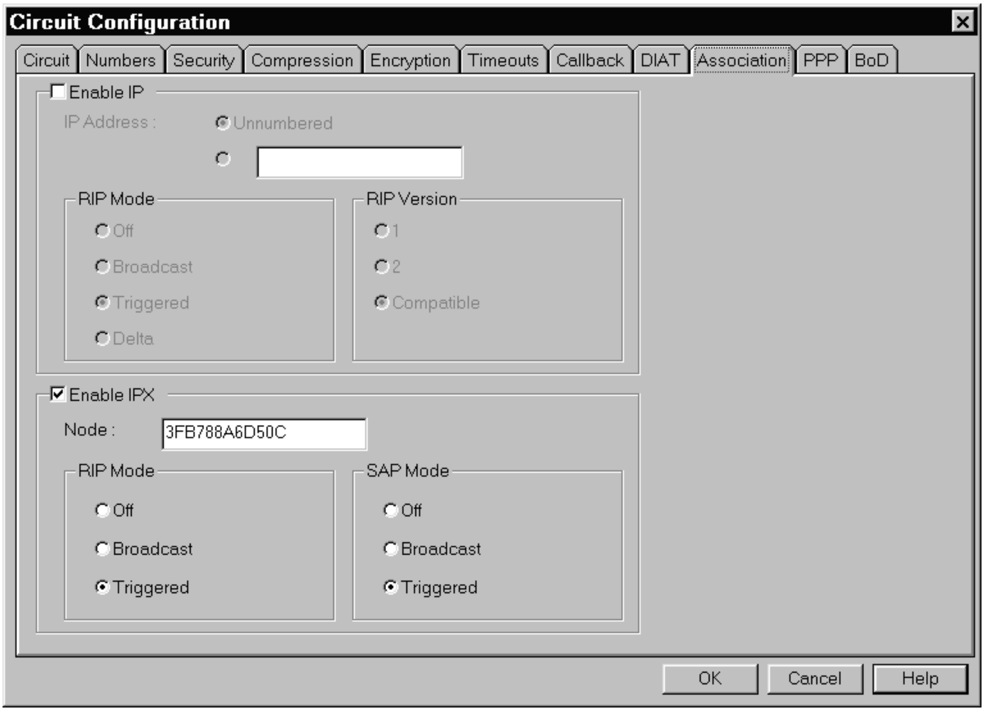
● Active
○ Inactive

4 If you want to use Triggered RIP on this circuit, then ensure that the Triggered RIP/SAP option is selected.

Note: You must enable Triggered RIP and SAP if you are using multiple static routes.

5 Click the Association tab.

Result: The Association tab appears.



□ Enable IP

IP Address : ● Unnumbered ○

RIP Mode: ○ Off ○ Broadcast ● Triggered ○ Delta

RIP Version: ○ 1 ○ 2 ● Compatible

☑ Enable IPX

Node : 3FB788A6D50C

RIP Mode: ○ Off ○ Broadcast ● Triggered

SAP Mode: ○ Off ○ Broadcast ● Triggered

6 Select RIP Mode as described in “RIP field descriptions” on page 307.

7 Click OK.

Result: The Data Circuit Add/Change/Remove screen appears.

8 Click OK again.

Result: You return to the Configuration tab.

RIP field descriptions

Field	Where	Description
Ignore Incoming RIP Updates	ISDN interface	Select this option if you are on a large network. When you select this option, the HomeOffice Router sends out routing information about itself but does not receive routing information. This reduces the number of routes that must be stored in the HomeOffice Router’s routing table.
Triggered Retry Count	ISDN interface	The triggered retry count defines the number of times that RIP tries to connect with RIP on the destination router if the Router cannot communicate (for example, if communications fail). Click Forever, or enter a value between 0 and 99. It is recommended you accept the default of 5.
Triggered Retry Interval	ISDN interface	The triggered retry interval defines the interval in minutes between triggered retry attempts. Enter a value between 1 and 10.
RIP Mode	ISDN circuit (Association tab)	In general, use Triggered over an ISDN connection, because this setting affects only this circuit, not the entire interface. About RIP modes • Off: RIP is off for the circuit, so you must create static routes. Use the IPX Routing table to do this. • Broadcast: RIP messages are sent every 60 seconds. If the link is not up, the link opens for these messages. • Triggered: RIP messages are sent only when the Routing table changes. If the link is not up, the link opens for these messages.

IPX Services and Service Advertising Protocol

Introduction

Service Advertising Protocol (SAP) is a protocol used by Novell Netware devices (such as printers, file servers, and gateways) to advertise their availability on the network by broadcasting their names, addresses, and current state.

The HomeOffice Router uses SAP to exchange service information with other routers and to update the information in its services table.

SAP is available on both the Ethernet and the ISDN interface. You may decide not to run SAP on the ISDN interface to reduce costs. However, you should keep SAP running on the Ethernet interface, because this does not affect connection costs.

Note: SAP is normally enabled along with RIP.

Configuration overview

Note: Review this section completely before beginning any configuration.

SAP

1 Enable SAP on the Ethernet interface (see page 311). SAP is enabled by default when configuring with the Install Wizard.

2 Configure SAP on the ISDN interface (see page 314).

3 Configure SAP on an ISDN circuit (see page 316).

IPX Services table

1 If SAP will not be enabled, configure the IPX Services table (see page 319).

2 Ensure that SAP is Off on the ISDN circuit (see page 316).

Types of SAP

Standard

Normally, you use SAP on a network to pass messages to other routers. When SAP operates in the standard way, messages are sent every 60 seconds. These messages tell the other routers that the source router is active and viable. This uses expensive ISDN bandwidth and causes unnecessary calls on wide area networks. Standard SAP is not recommended for ISDN.

Triggered

Triggered SAP is a method of keeping costs down on ISDN WANs. Triggered SAP is beneficial for more complex networks, where the configuration can change.

When Triggered SAP is used, the Router and other devices exchange SAP information when the Router is powered up. Instead of repeating this information, the Router and other devices do not exchange packets until the configuration changes. Configuration changes trigger update messages.

Triggered SAP gives you the benefit of dynamically updating service information without using excessive bandwidth. Update messages are sent only when the router detects a change in its service database. This means that service data is sent only when required, reducing ISDN usage and costs, while still being responsive to topology changes.

Note: If you set the ISDN address to call to DISABLED on a circuit, then you must also disable support for triggered RIP and SAP, as you cannot make outgoing calls on that circuit.

When to use SAP

Use SAP when

- service selection must happen quickly to prevent network congestion (the use of service tables can be time-consuming)
- you do not want to maintain service tables

On the Ethernet interface

Use SAP on the Ethernet interface if the telecommuter has created subnets (with the use of additional routers and bridges) on his or her own network.

On the ISDN interface

Use SAP on the ISDN interface if the telecommuter's LAN participates as an additional network (or series of subnets) recognized by the host network (DIAT is disabled). Under these circumstances, the HomeOffice Router receives regular updates on service information by any other SAP router on the same WAN subnet.

Benefits of SAP

On the Ethernet interface

When you use SAP on the Ethernet interface

- the HomeOffice Router can exchange SAP updates with routers (if present) on the same subnet of the telecommuter's LAN
- it is unnecessary to manually update the HomeOffice Router's service table

On the ISDN interface

When you use SAP on the ISDN interface

- the HomeOffice Router can exchange SAP updates with routers on the same WAN subnet of the host or central LAN
- it is unnecessary to manually update the HomeOffice Router's service table

Drawbacks of SAP

On the Ethernet interface

When you use SAP on the Ethernet interface, there is no significant reduction in performance, regardless of whether the telecommuter's network consists of additional subnets.

On the ISDN interface

You should carefully consider using SAP on the ISDN interface. The HomeOffice Router can be inundated with SAP broadcasts and result in repeated costly activation of the ISDN circuit and a significant reduction in network response time.

If the HomeOffice Router requires only a single service on the host network, a static entry for the service is recommended.

IPX Services table

Instead of confirming availability at frequent intervals (Broadcast SAP), you can configure service information statically in a services table. You must configure the services table at both ends of the link.

The IPX Service table lists up to 17 services that the HomeOffice Router can reach. You must configure the Service table if SAP is not enabled. Static entries are permanent and must be explicitly removed. Services do not time out.

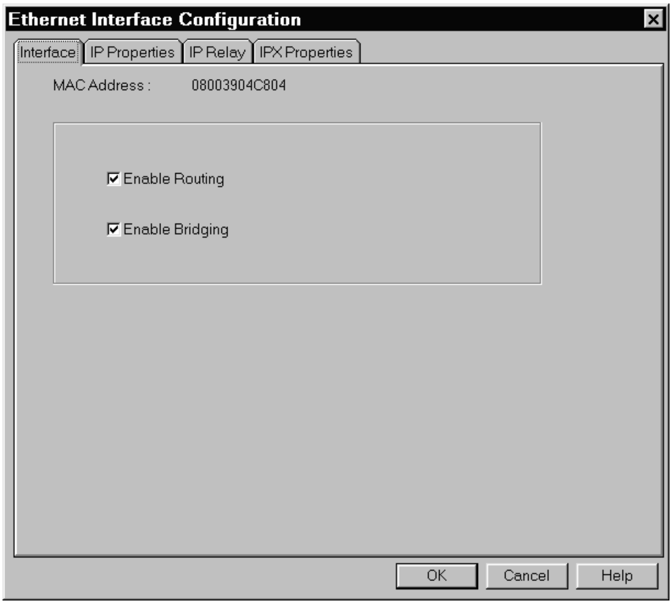
You can use the IPX Services table for less complex networks but doing so increases the amount of administration required for the network.

To enable SAP on the Ethernet interface

1 Click the Ethernet icon.

2 Select Properties from the pop-up menu that appears.

Result: The Ethernet Interface Configuration screen appears.



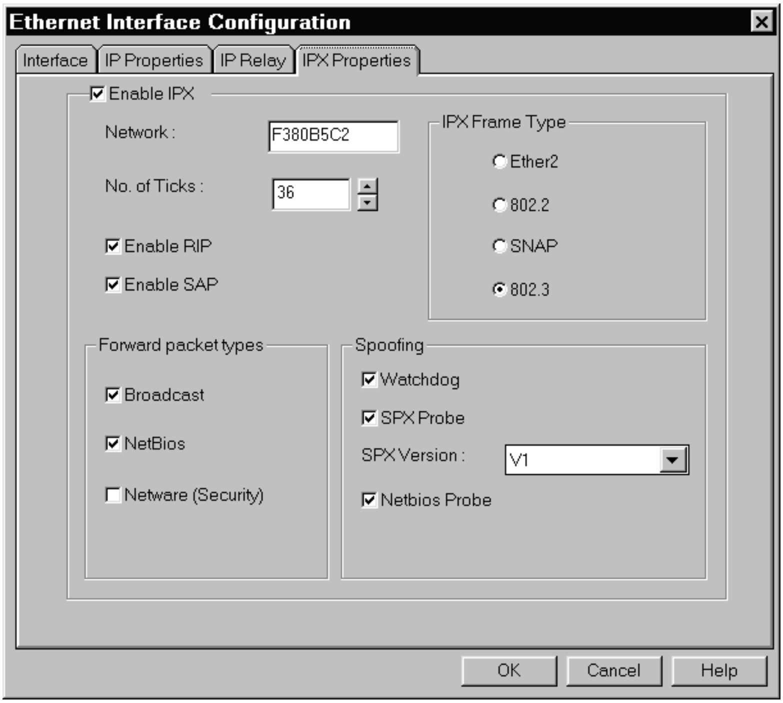
MAC Address : 08003904C804

☑ Enable Routing

☑ Enable Bridging

3 Click the IPX Properties tab.

Result: The IPX Properties tab appears.



Ethernet Interface Configuration

Interface | IP Properties | IP Relay | IPX Properties

☑ Enable IPX

Network : F380B5C2

No. of Ticks : 36

☑ Enable RIP

☑ Enable SAP

IPX Frame Type

○ Ether2

○ 802.2

○ SNAP

● 802.3

Forward packet types

☑ Broadcast

☑ NetBios

□ Netware (Security)

Spoofing

☑ Watchdog

☑ SPX Probe

SPX Version : V1

☑ Netbios Probe

4 Click Enable SAP.

5 Click OK.

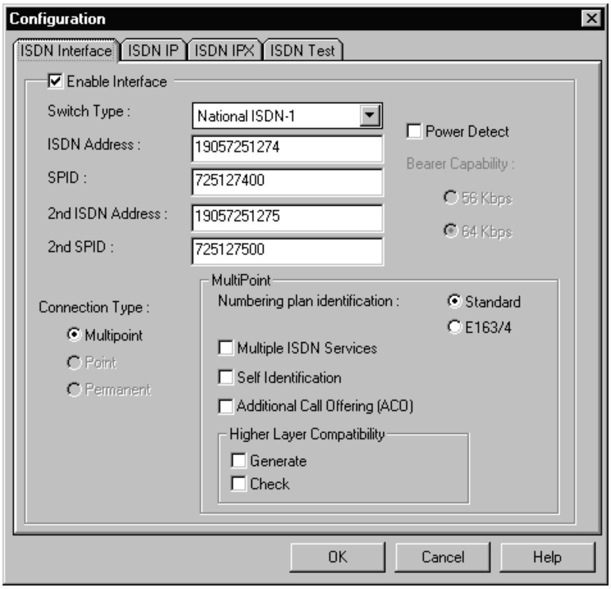
Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

To configure SAP on the ISDN interface

1 Click the ISDN icon.

2 Select Properties from the pop-up menu that appears.

Result: The Configuration screen appears.



Configuration

☑ Enable Interface

Switch Type : National ISDN-1

ISDN Address : 19057251274

SPID : 725127400

2nd ISDN Address : 19057251275

2nd SPID : 725127500

□ Power Detect

Bearer Capability :

○ 56 Kbps

● 64 Kbps

Connection Type :

● Multipoint

○ Point

○ Permanent

MultiPoint

Numbering plan identification : ● Standard ○ E163/4

□ Multiple ISDN Services

□ Self Identification

□ Additional Call Offering (ACO)

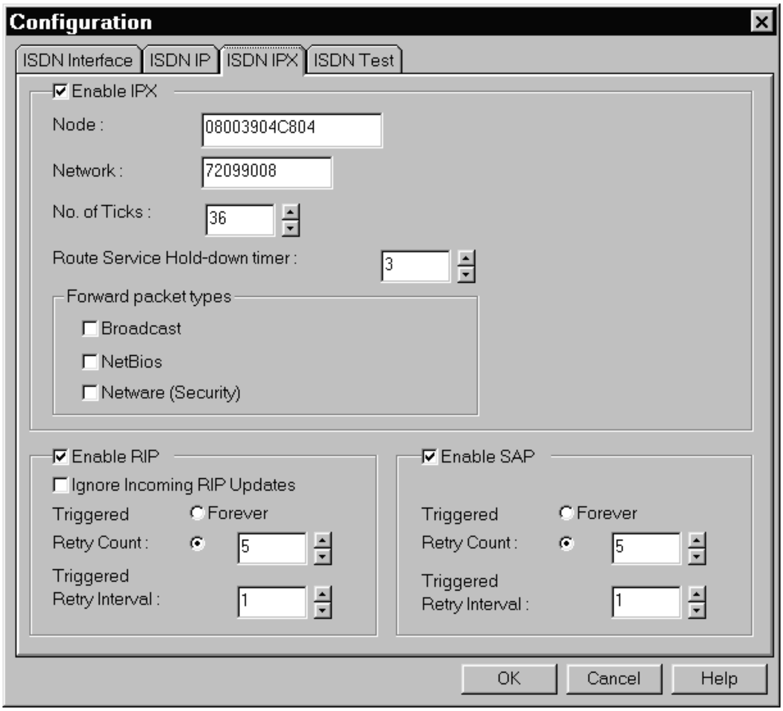
Higher Layer Compatibility

□ Generate

□ Check

3 Click the ISDN IPX tab.

Result: The ISDN IPX tab appears.



☑ Enable IPX

Node : 08003904C804

Network : 72099008

No. of Ticks : 36

Route Service Hold-down timer : 3

Forward packet types

□ Broadcast

□ NetBios

□ Netware (Security)

☑ Enable RIP

□ Ignore Incoming RIP Updates

Triggered Retry Count : ○ Forever ● 5

Triggered Retry Interval : 1

☑ Enable SAP

Triggered Retry Count : ○ Forever ● 5

Triggered Retry Interval : 1

4 Click Enable SAP.

5 Complete the fields as described in the “SAP field descriptions” on page 316.

6 Click OK.

Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

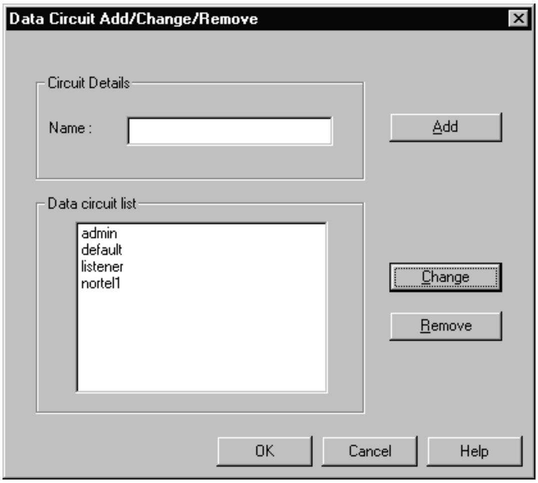
SAP field descriptions

Field	Description
Triggered Retry Count	The triggered retry count defines the number of times that SAP tries to connect with SAP on the destination router if the Router cannot communicate (for example, if communications fail). Click Forever, or enter a value between 0 and 99. The recommended value is 5.
Triggered Retry Interval	The triggered retry interval defines the interval in minutes between triggered retry attempts. Enter a value between 1 and 10.

To configure SAP on an ISDN circuit

1. Click the ISDN icon.
2. Select Circuits from the pop-up menu that appears.

   Result: The Data Circuit Add/Change/Remove screen appears.



Data Circuit Add/Change/Remove

Circuit Details

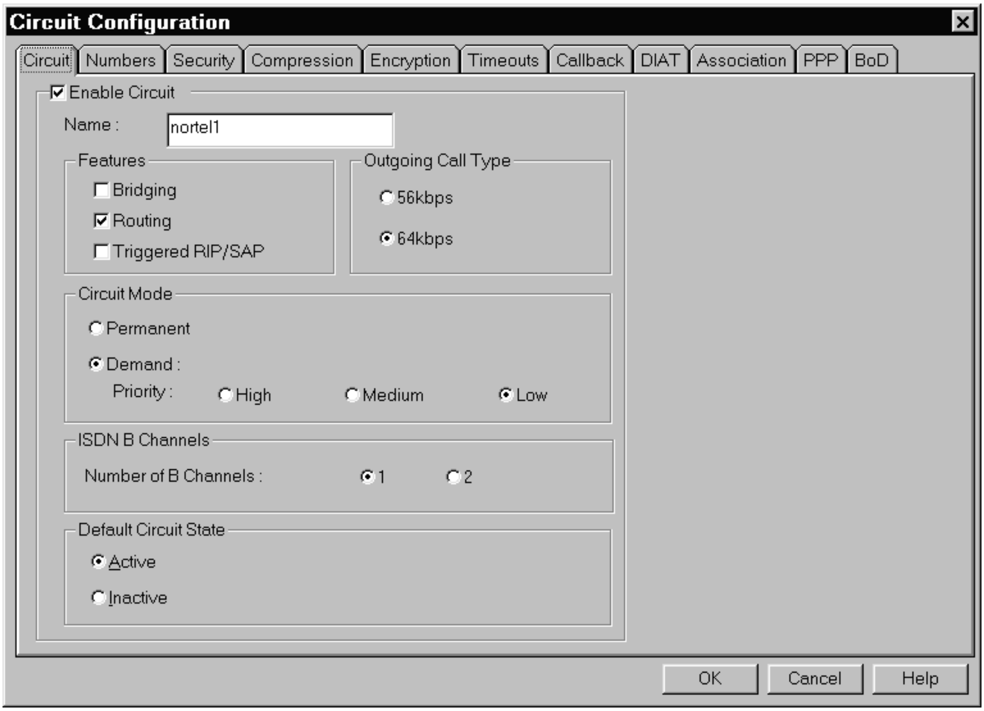
Name :

Data circuit list

admin
default
listener
nortel1

3 Select the circuit for which you want to configure SAP, and then click Change.

Result: The Circuit Configuration screen appears.



☑ Enable Circuit

Name : nortel1

Features

□ Bridging

☑ Routing

□ Triggered RIP/SAP

Outgoing Call Type

○ 56kbps

● 64kbps

Circuit Mode

○ Permanent

● Demand :

Priority : ○ High ○ Medium ● Low

ISDN B Channels

Number of B Channels : ● 1 ○ 2

Default Circuit State

● Active

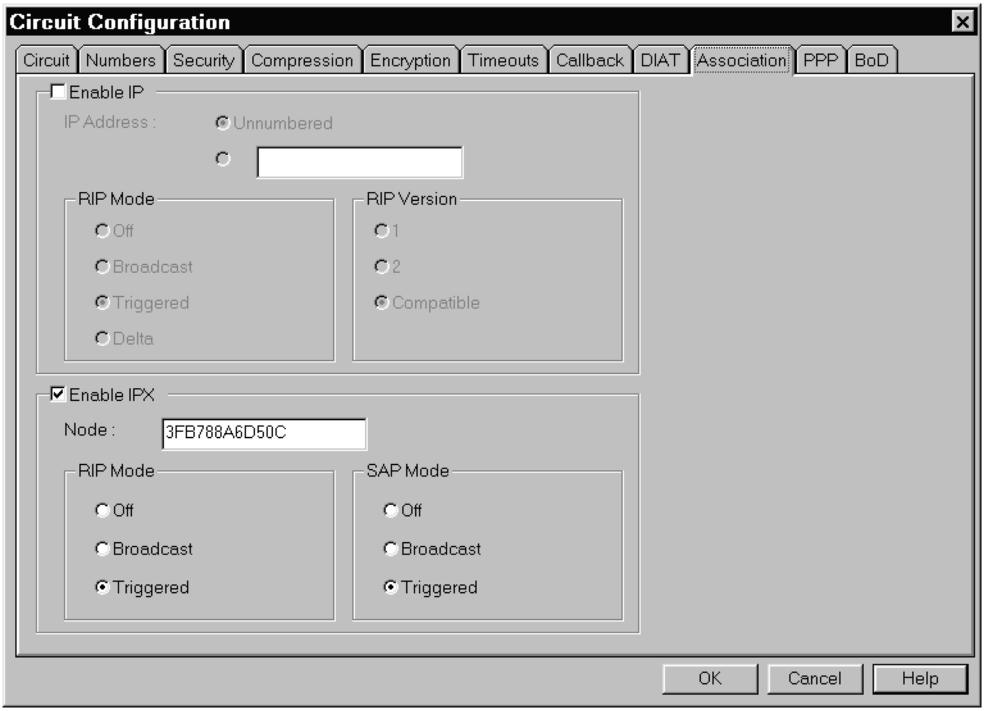
○ Inactive

4 If you want to use Triggered SAP on this circuit, then ensure that the Triggered RIP/SAP option is selected.

Note: You must enable Triggered RIP and SAP if you are using multiple static routes.

5 Click the Association tab.

Result: The Association tab appears.



☐ Enable IP

IP Address : ● Unnumbered ○

RIP Mode: ○ Off ○ Broadcast ● Triggered ○ Delta

RIP Version: ○ 1 ○ 2 ● Compatible

☑ Enable IPX

Node : 3FB788A6D50C

RIP Mode: ○ Off ○ Broadcast ● Triggered

SAP Mode: ○ Off ○ Broadcast ● Triggered

6 Select the SAP mode as follows:

- Off: SAP is off for the circuit, so you must set up services statically. Use the IPX Services table to do this.
- Broadcast: SAP messages are sent every 60 seconds. If the link is not up, the link opens for these messages.
- Triggered: SAP messages are sent only when the Services table changes. If the link is not up, the link opens for these messages. In general, use Triggered over an ISDN connection, because this setting affects only this circuit, not the entire interface.

7 Click OK.

Result: The Data Circuit Add/Change/Remove screen appears.

8 Click OK again.

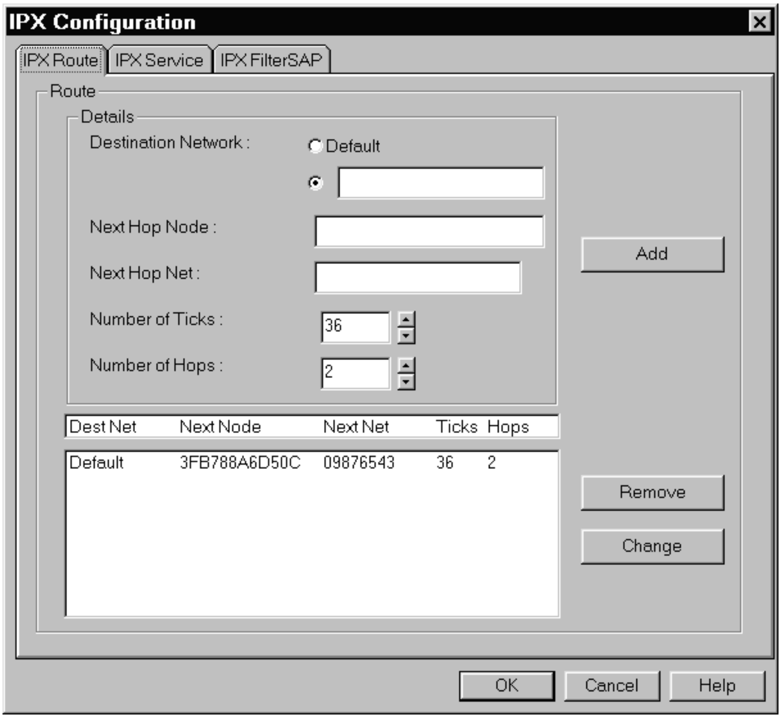
Result: You return to the Configuration tab.

To configure the IPX Services table

1 Click the Admin icon.

2 Select IPX Properties from the pop-up menu that appears.

Result: The IPX Configuration screen appears.



Destination Network : ○ Default ●

Next Hop Node :

Next Hop Net :

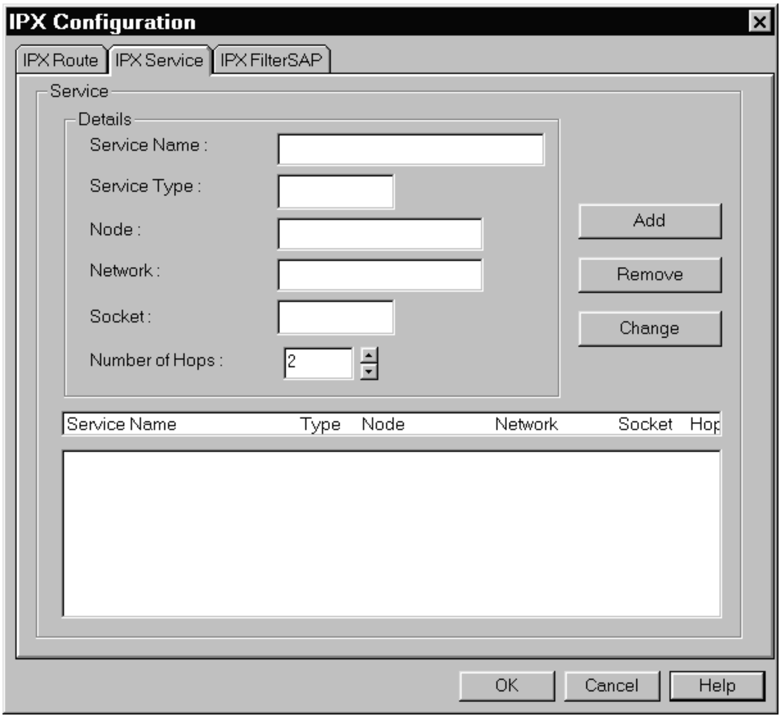
Number of Ticks : 36

Number of Hops : 2

Dest Net	Next Node	Next Net	Ticks	Hops
Default	3FB788A6D50C	09876543	36	2

3 Click the IPX Service tab.

Result: The IPX Service tab appears.



IPX Configuration

4 Complete the fields as described in “IPX Service table field descriptions” on page 321.

5 Click Add.

Result: The service is added to the table at the bottom of the screen.

6 Click OK.

Result: The IPX Service tab closes and you return to the Configuration tab.

IPX Service table field descriptions

Field	Description
Service Name	Enter the name of the service. It can be up to 20 characters in length and must be unique for that service type. **Note:** Service names are case-sensitive. For example, if you define *Printer1* as a service name and later type *printer1*, you will be unable to access this service.
Service Type	Enter a decimal value between 0 and 65535, indicating the type of service provided. The numbers and their corresponding services are defined by Novell. For example, the correct value for a file server is 4. For a print server, it is 7. Refer to your Novell system's documentation for a complete list of appropriate values. **Note:** The Service Name and the Service type must form a unique pair.
Node	Enter the node address of the device on which the service is located. This must be 12 hexadecimal digits in length.
Network	Enter the address of the network where the node providing the service is located. This must be 8 hexadecimal digits in length.
Socket	Enter the socket identifying the service. The value can be between 0 and 65535.
Number of Hops	Enter the number of routers that traffic must pass through to reach the destination network between 1 and 15. Normally, a workstation selects the service with the lowest number of hops. You can enter an artificially high or low number of hops to force clients to use (or not use) a particular service.

Filtering

Introduction

SAP filtering allows you to specify the IPX services that are not broadcasted to other network devices. You can apply filtering on either incoming or outgoing services on the Ethernet or ISDN interface.

When to use filtering

Use filtering when you do not want the HomeOffice Router to receive or send broadcasts for one or more IPX services on the Ethernet or ISDN interface.

Benefits of filtering

When you filtering service broadcasts, it reduces the amount of traffic over the ISDN interface.

Drawbacks of filtering

Filtered services are unavailable to other network users.

Filtering on the remote access switch

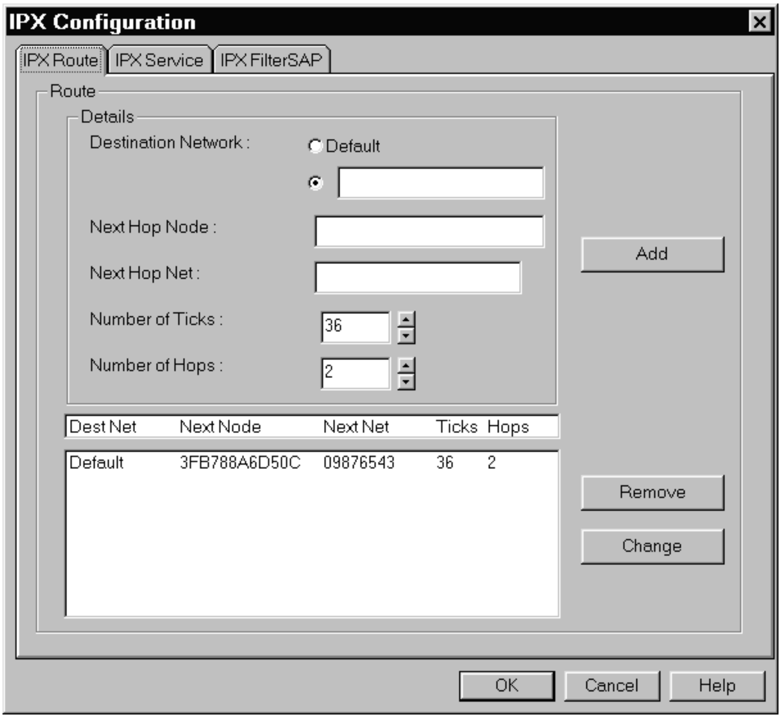
If filtering of SAP broadcasts is desired on the WAN link to HomeOffice Routers, It is recommended that as the first option (if possible), you implement SAP filtering at the remote access switch.

To configure the IPX SAP filtering table

1 Click the Admin icon.

2 Select IPX Properties from the pop-up menu that appears.

Result: The IPX Configuration screen appears.



Destination Network : ○ Default ●

Next Hop Node :

Next Hop Net :

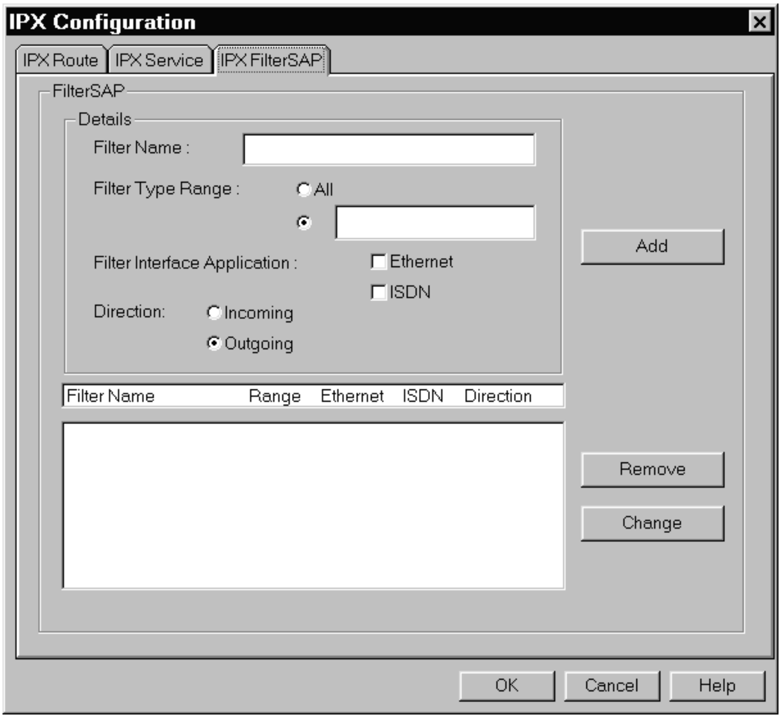
Number of Ticks : 36

Number of Hops : 2

Dest Net	Next Node	Next Net	Ticks	Hops
Default	3FB788A6D50C	09876543	36	2

3 Click the IPX FilterSAP tab.

Result: The IPX FilterSAP tab appears.



Filter Type Range : ○ All ●

Filter Interface Application : □ Ethernet □ ISDN

Direction: ○ Incoming ● Outgoing

4 Complete the fields as described in “IPX SAP filtering table fields descriptions” on page 325.

5 Click Add.

Result: The filter is added to the table at the bottom of the screen.

6 Click OK.

Result: The IPX FilterSAP tab closes and you return to the Configuration tab.

IPX SAP filtering table fields descriptions

Field	Description
Filter Name	Enter a name for the filter that you want to add. This name can be up to 15 characters long.
Filter Type Range	Click ALL if you do not want to forward information on any services. If you want to forward information on some services, click Filter Type Range and then enter the number or range of IPX services that you do not want to be forwarded to other devices.
Filter Interface Application	Use this option to choose whether you want these filters to apply to the LAN or WAN, or both. Select Ethernet if you want these filters to apply to the LAN. Select ISDN if you want these filters to apply to the WAN. **Note:** This option is grayed out if you choose to filter incoming services.
Direction	Use this option to choose whether you want to filter Incoming or Outgoing Services. **Note:** If you select Incoming, the Filter Interface Application option is not relevant. Therefore, it is grayed out.

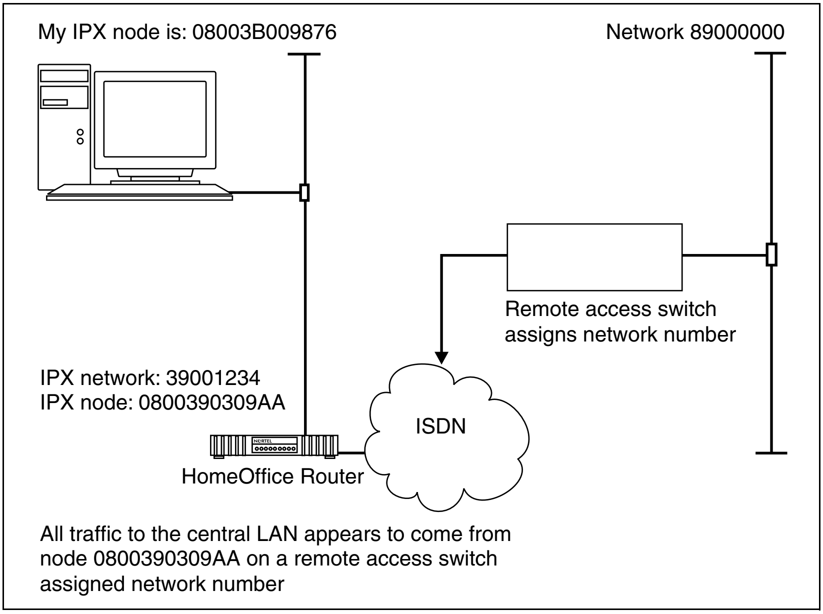
Dynamic IPX Address Translation

Introduction

Dynamic IPX Address Translation (DIAT for IPX) is a mechanism by which a remote network of one or more devices can appear as a single device to the host network. This allows the remote network the flexibility to implement an addressing scheme that is invisible to the host network.

How DIAT for IPX works

ISG605_I


My IPX node is: 08003B009876
Network 89000000
Remote access switch assigns network number
IPX network: 39001234
IPX node: 0800390309AA
ISDN
HomeOffice Router
All traffic to the central LAN appears to come from node 0800390309AA on a remote access switch assigned network number

The HomeOffice Router is shipped with a default IPX node number. This number can remain when using DIAT for IPX.

Configure the PC with an address on the same LAN as the HomeOffice Router. In this example, the PC’s network number (IPX network) is 39001234. When the telecommuter calls an application that requires a network connection, the HomeOffice Router calls the central site and receives a dynamically assigned IPX network number.

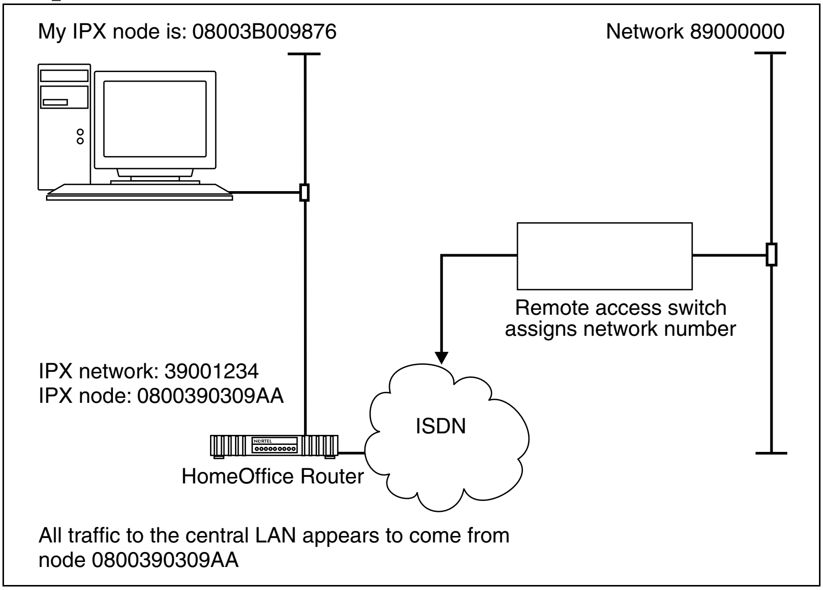
The HomeOffice Router then translates the PC's address to the dynamically assigned IPX address. Note that the PC's own address is never seen outside of its own LAN.

Single-host DIAT for IPX

Single-host DIAT for IPX simplifies the configuration of the HomeOffice Router for telecommuters who regularly access a network from different locations. For example, a telecommuter with a portable computer can access the corporate network with the same configuration as the one used to connect the home office to the corporate headquarters.

The following illustration shows how a telecommuter with a single PC is connected to the local network.

ISG631_I


My IPX node is: 08003B009876
Network 89000000
Remote access switch assigns network number
IPX network: 39001234
IPX node: 0800390309AA
ISDN
HomeOffice Router
All traffic to the central LAN appears to come from node 0800390309AA

The central remote access switch gives the HomeOffice Router. The HomeOffice Router uses this network number to communicate with the central site.

However, when the HomeOffice Router is communicating with the local network, it uses a different IPX network address. The HomeOffice Router's Ethernet interface and the device (in this case, the telecommuter's PC) have addresses on that network.

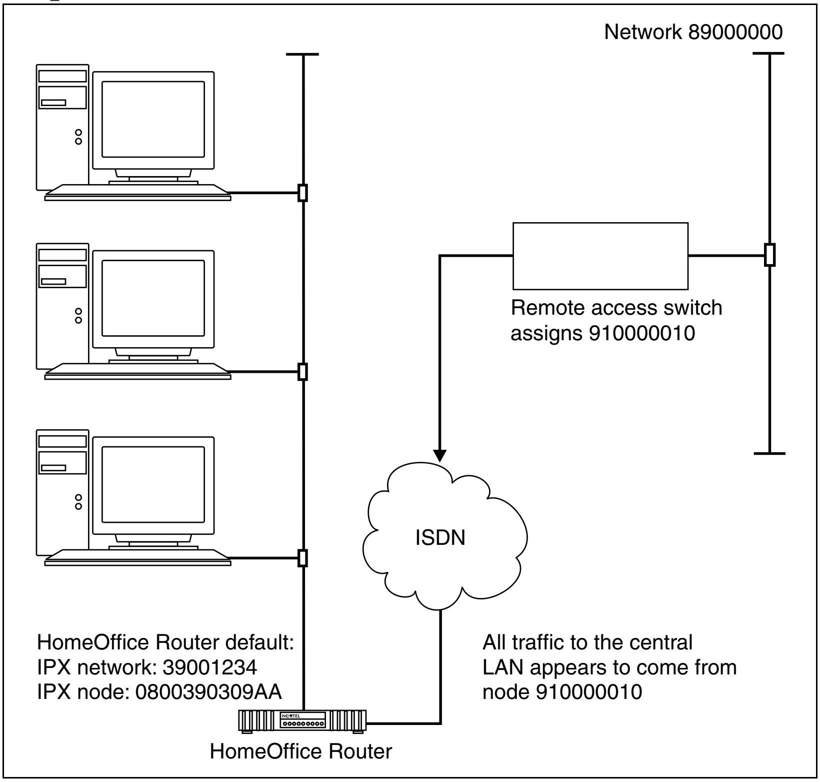
Therefore, in this example, the HomeOffice Router communicates with the LAN on the 39001234 network, but it communicates with the remote site over the WAN using the address that has been invisibly assigned to it by the remote access switch.

Multi-host DIAT for IPX

Use multi-host DIAT for IPX when there is more than one device on the remote LAN. With multi-host DIAT for IPX, the HomeOffice Router provides IPX Socket Translation (as well as IPX Address Translation). This ensures that packets are returned to the correct device. The remote LAN still appears as a single device to the central site. See the following illustration.

A key advantage of multi-host DIAT for IPX is that all the remote sites can be given the same configuration at one time by a network manager.

ISG610_I



DIAT for IPX features

DIAT for IPX provides the following features:

- dynamic address discovery

  A network address for the telecommuter is obtained from the IPX-based host network and assigned to the HomeOffice Router.

- address translation

  The source address of outbound data from a remote network device is translated to the address of the HomeOffice Router. To the host network, any data that originates from a device on the remote network appears as if it originates from the HomeOffice Router.

Conversely, data from the host network that is destined for a remote device is given the address of the HomeOffice Router. The HomeOffice Router translates this address to the remote network address of the destination device and routes the data.

The address translation that occurs is transparent to both the remote and host networks.

- port translation for remote networks with multiple devices

  IPX socket translation is used to ensure that packets are routed to the correct remote device.

Benefits

DIAT for IPX provides the following significant benefits:

- You can use IP and IPX on the same circuit, provided that both are set for DIAT or for LAN-to-LAN.
- When using DIAT for IPX, the HomeOffice Router can fully participate in very large, corporate IPX networks.

  The only restriction is that your LAN cannot offer services to an IPX network. Without DIAT for IPX, the HomeOffice Router can only access a limited number of services.
- You save valuable address space assignment to remote network devices.
- Remote network addressing is flexible.

Drawbacks

If more than ten hosts share an IPX address, then this can cause a degradation in performance due to ISDN bandwidth limitations.

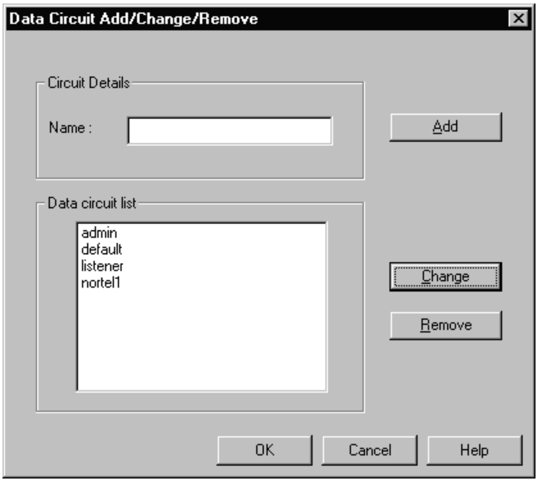
When to use DIAT for IPX

Enable DIAT for IPX if the NetWare network assigns network numbers or addresses to telecommuters.

To enable DIAT for IPX on a circuit

1. Click the ISDN icon.
2. Select Circuits from the pop-up menu that appears.

   Result: The Data Circuit Add/Change/Remove screen appears.



Data Circuit Add/Change/Remove

Circuit Details

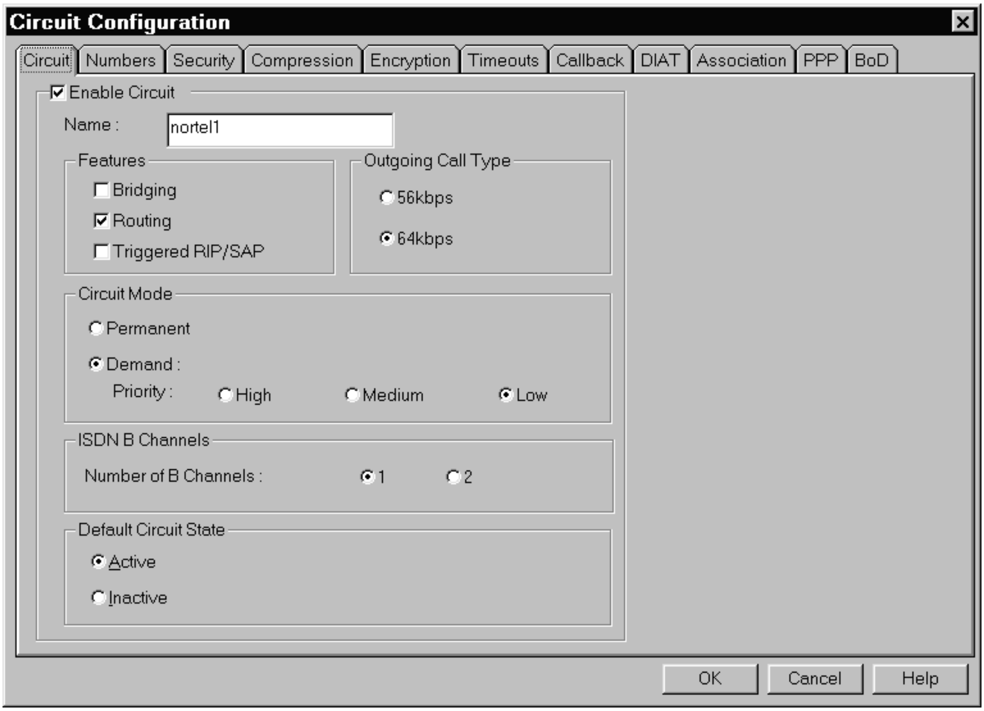
Name :

Data circuit list

admin
default
listener
nortel1

3. Select the circuit for which you want to enable DIAT for IPX, and then click Change.

   Result: The Circuit Configuration screen appears.



☑ Enable Circuit

Name : nortel1

Features

☐ Bridging

☑ Routing

☐ Triggered RIP/SAP

Outgoing Call Type

○ 56kbps

● 64kbps

Circuit Mode

○ Permanent

● Demand :

Priority : ○ High ○ Medium ● Low

ISDN B Channels

Number of B Channels : ● 1 ○ 2

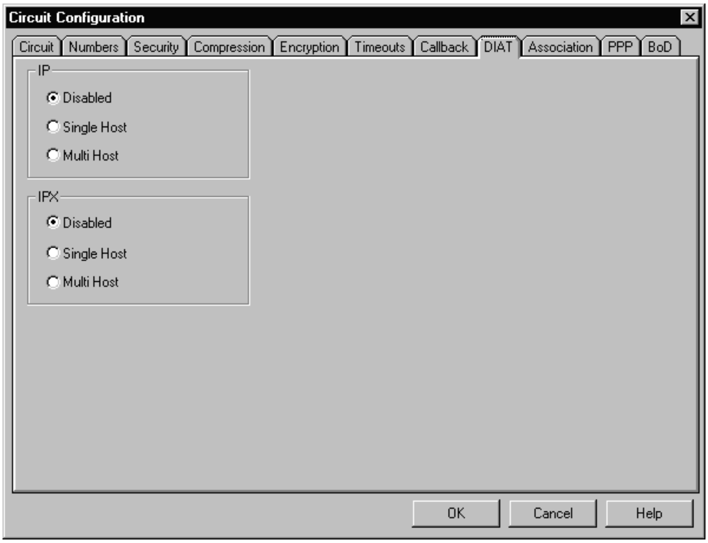
Default Circuit State

● Active

○ Inactive

4 Click the DIAT tab.

Result: The DIAT tab appears.



IP

● Disabled

○ Single Host

○ Multi Host

IPX

● Disabled

○ Single Host

○ Multi Host

5 In the IPX area, do one of the following:

- Click Single Host if only the PC will be sharing an IPX address with the HomeOffice Router.
- Click Multi Host if the PC and one or more other devices will be sharing an IPX address with the HomeOffice Router.

6 Click OK.

Result: The Data Circuit Add/Change/Remove screen appears.

7 Click OK again.

Result: You return to the Configuration tab.

Broadcast Forwarding

Introduction

A broadcast is a network transaction that sends data to one or more hosts connected to the network.

Configuration overview

Note: Review this section completely before beginning any configuration.

On the Ethernet interface

Specify the IPX frame type and the types of network packets that should be forwarded to the network (see page 335).

On the ISDN interface

Specify the types of network packets that should be forwarded to the remote network (see page 338).

Frame type

The HomeOffice Router must use the same frame type as the servers and workstations on the LAN to communicate with them.

The IPX frame type can be configured only on the Ethernet interface. Possible values are

- ETHER2: IPX uses a unique packet header (type code). This value is suitable for networks that involve Digital Equipment Corporation networking or the TCP/IP protocol.
- 802.2: The HomeOffice Router uses the IEEE and OSI standard 802.2 frame type.

  Note: 802.2 is the default value.

- SNAP: The HomeOffice Router uses the IEEE and OSI standard 802.2 frame type with the 802.2 SNAP extension.
- 802.3: The HomeOffice Router uses a standard Novell frame on a network that uses only NetWare.

Forward packet types

You can forward the following types of networking packets to the remote network:

- broadcast
- NetBIOS
- NetWare security packets

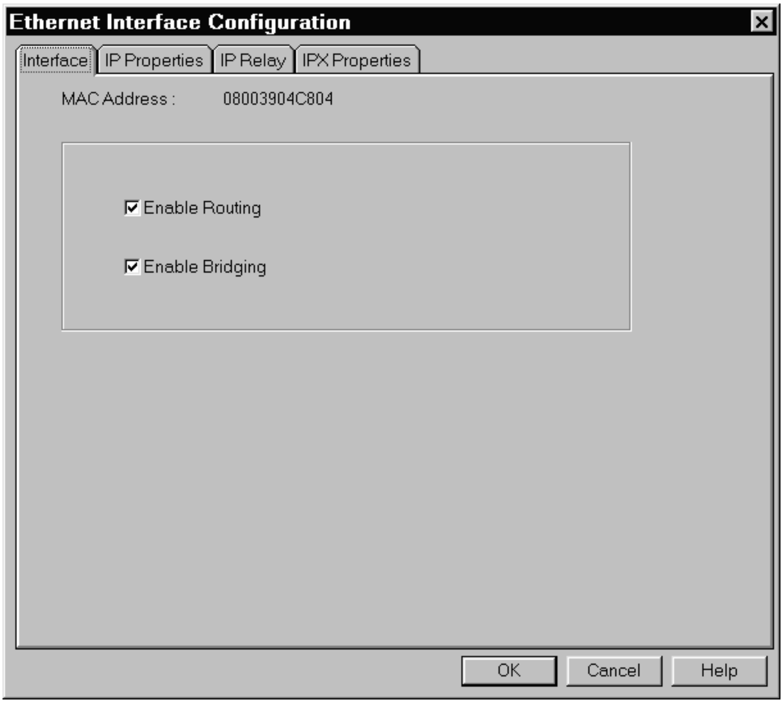
Novell servers that know about each other exchange security packets every 60 seconds, which can increase ISDN costs considerably. By default, the HomeOffice Router does not forward security packets, which stops them from being sent over your ISDN link.

It is recommended that you do not enable forwarding of NetWare security packets.

To select the IPX frame and forward packet types on the Ethernet interface

1. Click the Ethernet icon.

   Result: The Ethernet Interface Configuration screen appears.



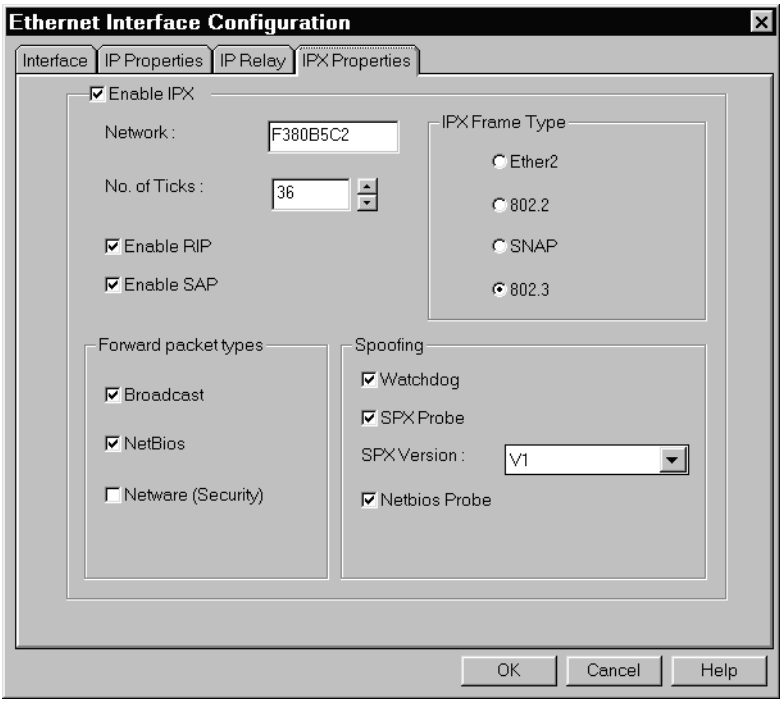
MAC Address : 08003904C804

☑ Enable Routing

☑ Enable Bridging

2 Click the IPX Properties tab.

Result: The IPX Properties tab similar to the following appears.



☑ Enable IPX

Network : F380B5C2

No. of Ticks : 36

☑ Enable RIP

☑ Enable SAP

IPX Frame Type

○ Ether2

○ 802.2

○ SNAP

● 802.3

Forward packet types

☑ Broadcast

☑ NetBios

□ Netware (Security)

Spoofing

☑ Watchdog

☑ SPX Probe

SPX Version : V1

☑ Netbios Probe

3 Select the IPX Frame Type.

Note: See “Frame type” on page 334 for a description of the options.

4 Select the options that you need under Forward packet types.

Note: See “Forward packet types” on page 335 for more information.

5 Click OK.

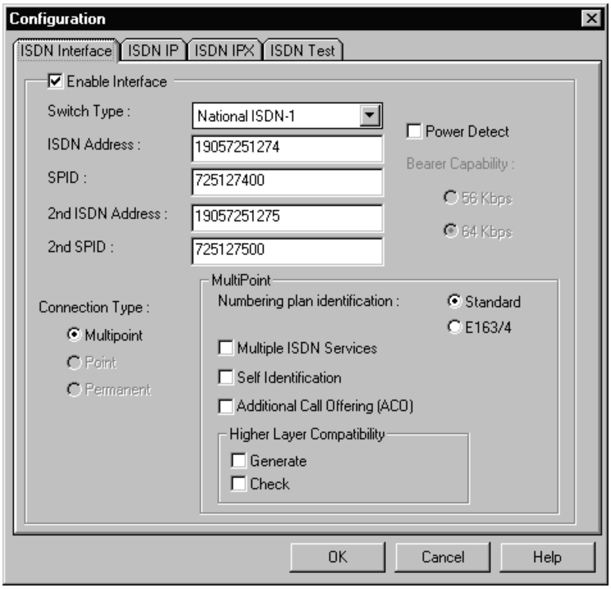
Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

To specify the forward packet types on the ISDN interface

1 Click the ISDN icon.

2 Select Properties from the pop-up menu that appears.

Result: The Configuration screen appears.



☑ Enable Interface

Switch Type : National ISDN-1

ISDN Address : 19057251274

SPID : 725127400

2nd ISDN Address : 19057251275

2nd SPID : 725127500

□ Power Detect

Bearer Capability :

○ 56 Kbps

● 64 Kbps

Connection Type :

● Multipoint

○ Point

○ Permanent

MultiPoint

Numbering plan identification : ● Standard ○ E163/4

□ Multiple ISDN Services

□ Self Identification

□ Additional Call Offering (ACO)

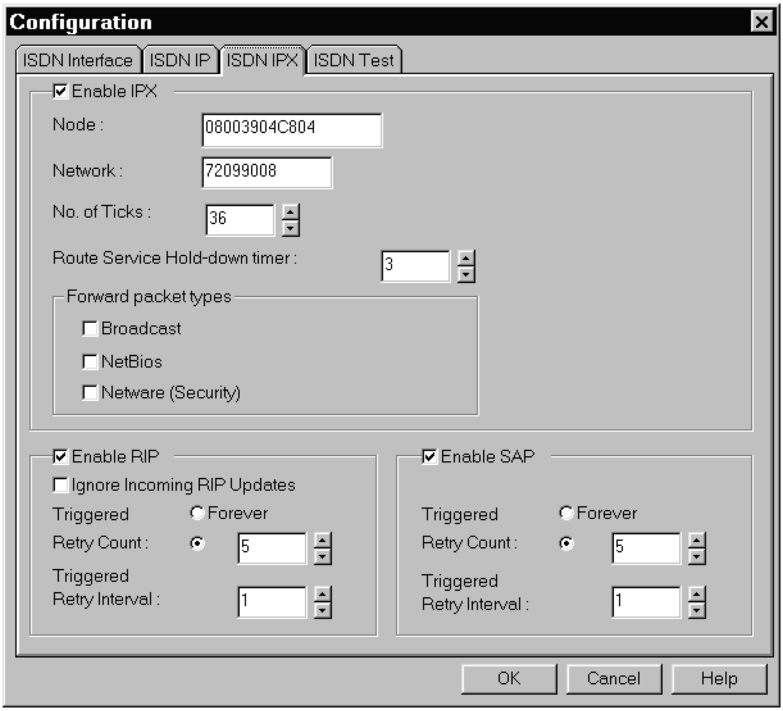
Higher Layer Compatibility

□ Generate

□ Check

3 Click the ISDN IPX tab.

Result: The ISDN IPX tab appears.



☑ Enable IPX

Node : 08003904C804

Network : 72099008

No. of Ticks : 36

Route Service Hold-down timer : 3

Forward packet types

□ Broadcast

□ NetBios

□ Netware (Security)

☑ Enable RIP

□ Ignore Incoming RIP Updates

Triggered ○ Forever

Retry Count : ● 5

Triggered Retry Interval : 1

☑ Enable SAP

Triggered ○ Forever

Retry Count : ● 5

Triggered Retry Interval : 1

4 Select the options that you need under Forward packet types.

Note: See “Forward packet types” on page 335 for more information.

5 Click OK.

Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

Spoofing

Introduction

Spoofing is the process by which the HomeOffice Router prevents meaningless traffic from keeping the network connection open. The Ethernet interface settings control some kinds of IPX spoofing that the HomeOffice Router performs. This lets you determine, for some kinds of network traffic, whether the packets are meaningful.

Configuration overview

Note: Review this section completely before beginning any configuration.

Enable or disable spoofing types on the Ethernet interface (see page 342).

How it works

When you open a connection to a remote network, the computer and other devices on the local and remote networks send a constant stream of network traffic that can keep the network connection open, even when you are not using it for a specific purpose.

It can be expensive to keep the network connection open, so the HomeOffice Router closes the connection during idle periods, which are defined as times when no meaningful network traffic is flowing between the local and remote networks.

The spoofing configuration defines the type of traffic that *should not* be sent (therefore, making the traffic meaningless).

Types of spoofing

You can enable the following types of spoofing:

- watchdog spoofing

  This method keeps costs down by sending spoof packets from a router on a LAN to another router on the same network. These packets simulate the keep-alive packets normally sent across a WAN from a workstation to the router, to maintain the connection. Since the packets are sent locally, the transmission costs are lower.

- SPX probe spoofing

  SPX probe spoofing is based on a similar principle to IPX watchdog spoofing, but it is done on a different type of frame, and in both directions. SPX probe spoofing significantly reduces network costs because probe packets are responded to locally by the router and are not sent across the WAN link. When an SPX connection between a server and client is idle, packets are sent from the server to the client, and vice versa, to ensure that the connection is still there.

  If you enable SPX probe spoofing, you must also select the version of SPX spoofing to be used. The choices are V1, V2, or Piggyback.

  It is recommended that you use Piggyback so that the packets are spoofed only when a call is not open and are passed as normal when a call is open. You must use the same version of spoofing at both ends of the link, so check with the network administrator if you are not sure which version is in use on the central LAN.

- NetBIOS probe spoofing

  This is used to spoof NetBIOS probe packets.

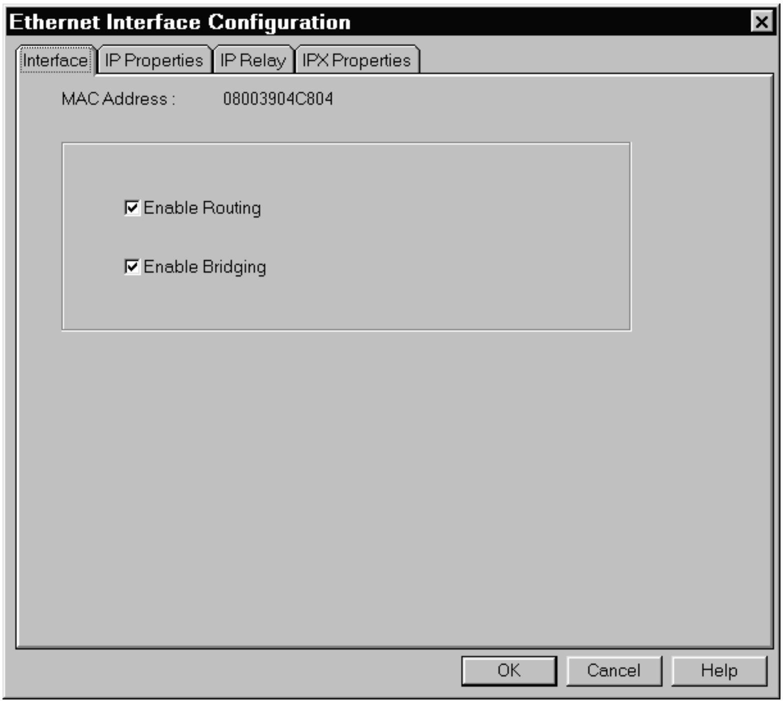
When to use spoofing

Use spoofing if you want to reduce ISDN line usage costs.

To enable spoofing types on the Ethernet interface

1 Click the Ethernet icon.

Result: The Ethernet Interface Configuration screen appears.



Ethernet Interface Configuration

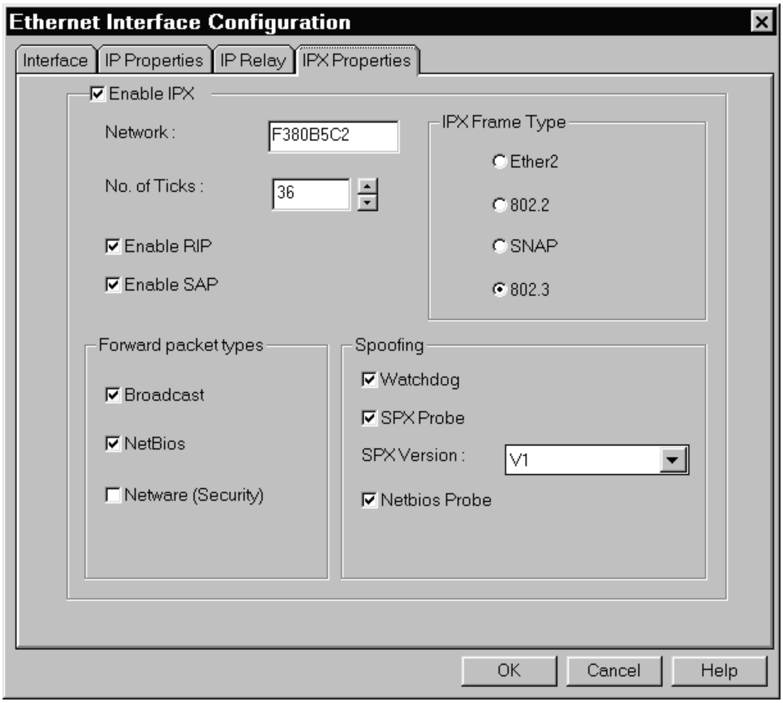
MAC Address : 08003904C804

☑ Enable Routing

☑ Enable Bridging

2 Click the IPX Properties tab.

Result: The IPX Properties tab appears.



☑ Enable IPX

Network : F380B5C2

No. of Ticks : 36

☑ Enable RIP

☑ Enable SAP

IPX Frame Type

○ Ether2

○ 802.2

○ SNAP

● 802.3

Forward packet types

☑ Broadcast

☑ NetBios

□ Netware (Security)

Spoofing

☑ Watchdog

☑ SPX Probe

SPX Version : V1

☑ Netbios Probe

3 Select the spoofing options you want to use.

Note: For more information, see “Types of spoofing” on page 341.

4 Click OK.

Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

IPX Bridging

Introduction

Bridging offers one of the most straightforward and flexible methods of interconnecting network segments. Bridges are very simple to use. Existing applications or communications software require no changes when bridges are introduced to a network.

If you set up your device as a bridge/router, then IPX is routed across the interfaces that have the IPX protocol enabled, while all other protocols (DECnet, AppleTalk, Banyan Vines, SNA, and so on) are bridged.

Configuration overview

Note: Review this section completely before beginning any configuration.

1. Enable Bridging on the Ethernet interface (see page 346).
2. Configure a bridge (see page 347).

When to use IPX bridging

Use IPX bridging if telecommuters require the NetWare Link Service Protocol (NLSP) for the network connection.

Benefits

With most bridges, you must only connect them to your network and turn them on. A bridge

- automatically learns the addresses of all active stations on its LAN
- examines all the packets on the LAN, reading their source and destination addresses
- forwards packets destined for a remote network to that network, over the WAN
- ignores or filters packets running between addresses on the local network

This means that traffic intended only for the local segment does not cross the bridge and clutter up the rest of the network.

Drawbacks and workaround

The bridge must forward some packets, such as broadcasts, multicasts, and packets with unknown destinations, across the WAN to all parts of the network. This can cause the following problems when bridging across ISDN:

- If you have configured more circuits than you have B-channels, the bridge tries to transmit broadcast and multicast packets, and packets with unknown destinations on all circuits. However, transmission has to be complete on the first two circuits before more circuits can be opened. As a result, transmission is delayed on some circuits, or packets are discarded.
- Every broadcast and multicast transmission, or transmission to an unknown destination results in an ISDN call. Every call costs money.

The solution to both of these problems is to set up filtering to control the amount of traffic sent across ISDN links.

Filtering

Filtering is the process of testing whether a packet must be passed onto another network segment. It is designed to decrease the level of traffic on your network and is cost-effective because it eliminates most unnecessary traffic between networks.

You can set up filters based on the destination and source addresses of packets, access groups, packet type, and data content of packets. This helps to reduce the level of traffic passing over the ISDN link or prevents certain users from accessing the ISDN link.

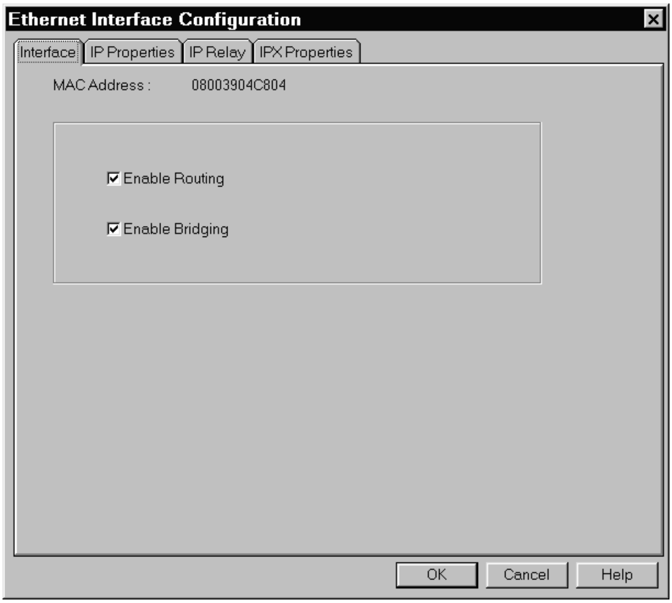
To configure the Router for bridge filtering, use the `bridge filter` command in the HomeOffice Router command shell. For instructions, refer to the *Meridian HomeOffice II Command Shell User Guide* (NTP 555-8321-910) on the Meridian HomeOffice II CD-ROM.

To enable Bridging on the Ethernet interface

1 Click the Ethernet icon.

2 Select Properties from the pop-up menu that appears.

Result: The Ethernet Interface Configuration screen appears.



MAC Address : 08003904C804

☑ Enable Routing

☑ Enable Bridging

3 Ensure that the Enable Bridging check box is checked.

4 Click OK.

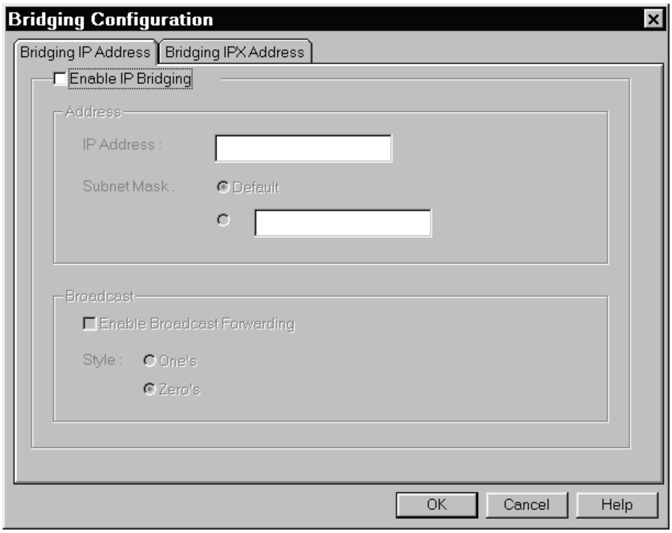
Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

To configure a bridge

1 Click the Admin icon.

2 Select Bridging from the pop-up menu that appears.

Result: The Bridging Configuration screen appears.



Bridging Configuration

Bridging IP Address | Bridging IPX Address

□ Enable IP Bridging

Address

IP Address :

Subnet Mask : ● Default

○

Broadcast

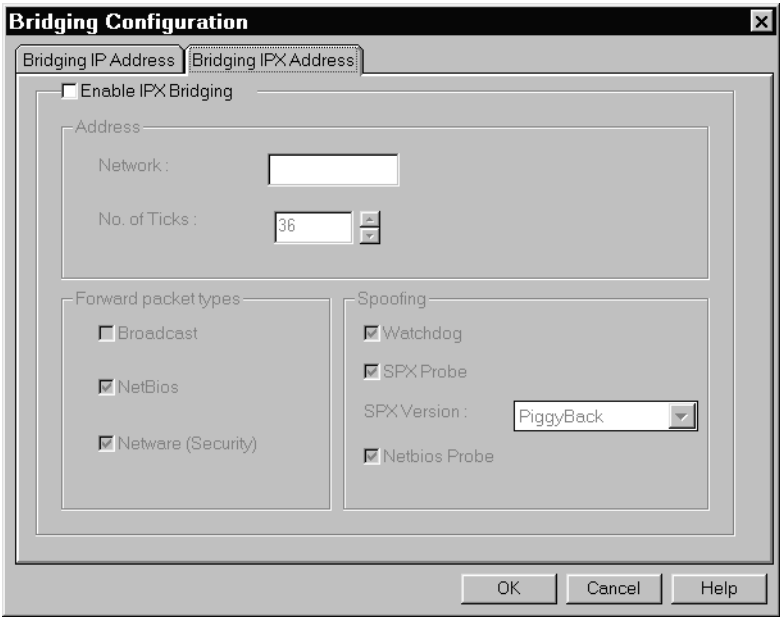
□ Enable Broadcast Forwarding

Style : ○ One's

● Zero's

3 Click the Bridging IPX Address tab.

Result: The Bridging IPX Address tab appears.



Bridging Configuration

☐ Enable IPX Bridging

Address

Network :

No. of Ticks : 36

Forward packet types

☐ Broadcast

☑ NetBios

☑ Netware (Security)

Spoofing

☑ Watchdog

☑ SPX Probe

SPX Version : PiggyBack

☑ Netbios Probe

4 Complete the fields as described in “Bridging IPX Address field descriptions” below.

5 Click OK.

Result: A message appears indicating that the Router is being reconfigured. When reconfiguration is completed, your connection is reestablished with the Router.

Bridging IPX Address field descriptions

Field	Description
Enable IPX Bridging	Select this option if you want to activate or deactivate IPX for bridging interfaces. **Note:** The change does not take effect until you restart your Router.
Network	Enter the IPX address of the network to which the Router is attached. **Warning:** If you delete the IPX network address from the Network field, deselect the Enable IPX check box and click OK: this resets *all* of your IPX Bridging configuration.
No. of Ticks	The number of ticks is a measure of the time necessary to deliver a 576-byte packet to a node on that network in 1/18ths of a second. For wide area links, the time depends upon the line speed and how busy the line is. Values should be long and never shorter than 2 seconds (36 ticks). The fastest value you should set for ISDN is 5/18ths of a second (5 or 6 ticks). Enter a value between 1 and 65535. If the destination is reached over the Ethernet interface, set the value to 1.
Forward packet types	Select the kind of networking packets that you want forwarded to the remote network. For more information, see “Forward packet types” on page 335.
Spoofing	Select the types of spoofing that you want to use. For more information, see “Types of spoofing” on page 341.

Chapter 4

Administration

In this chapter

Overview

Introduction

Once you have completed HomeOffice Router deployment, you must maintain the network. This chapter provides a description of some suggested administration activities.

Connections to remote sites

You can establish a connection to a remote HomeOffice Router by

- a remote LAN-to-LAN connection
- Ethernet
- Telnet

Upgrades

Nortel Networks continually works on Meridian HomeOffice II to improve its functionality, and posts product updates on the Nortel Networks web page. You must ensure that the current firmware and software are installed to use new features that have been added.

Administration

Miscellaneous but important administration activities include the following:

- backups and restores
- reassigning Routers
- changing the Meridian password
- returning components for repair

Section A: Connecting to remote sites

In this section

Overview

Introduction

You can establish a connection to a remote HomeOffice Router by

- a remote LAN-to-LAN connection
- Ethernet
- Telnet

Remote LAN-to-LAN connection

Before you can establish a connection with a telecommuter’s Router over ISDN, you must perform the configuration described in “Configuring the HomeOffice Router for remote administration” on page 124.

Connection over Ethernet

To establish a connection over Ethernet:

- IP connectivity must exist between the PC with Local Manager and the remote HomeOffice Router over the Ethernet interface.
- You need to know the IP address of the remote HomeOffice Router.

Connection with Telnet

You can use the Windows Telnet program to access the HomeOffice Router command shell. You only use Telnet access for administrative functions performed in the HomeOffice Router command shell. When you quit the command shell, the Telnet connection is dropped.

The administration PC must be connected to the HomeOffice Router by Ethernet.

Establishing a remote LAN-to-LAN connection

Introduction

This procedure describes how to access a HomeOffice Router to perform remote administration, upgrades, or both. Use this method if you want to perform remote administration over ISDN instead of Ethernet.

Before you begin

Before you can establish a connection with a telecommuter’s Router over ISDN, you must perform the configuration described in “Configuring the HomeOffice Router for remote administration” on page 124.

Note: The “Administration tips” on page 124 provide suggestions on what to do if you must perform administration on more than 14 remote Routers.

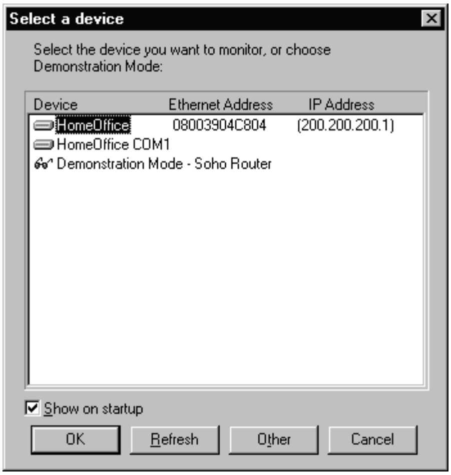
To connect to the remote Router over ISDN

1 Verify that the remote Router that you want to access is not already being monitored through the telecommuter’s Local Manager software (if this privilege has been granted to the telecommuter).

Only one administrative connection to the device can be active at a time. Before you attempt to connect to the remote Router, ask the telecommuter to click Edit, and then select Stop monitoring.

2 On the administration Router, click ☰ (or select Edit > Select device).

Result: The Select a device screen appears.



Select a device

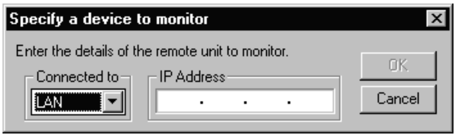
Select the device you want to monitor, or choose Demonstration Mode:

Device	Ethernet Address	IP Address
HomeOffice	08003904C804	(200.200.200.1)
HomeOffice COM1		
Demonstration Mode - Soho Router		

☑ Show on startup

3 Click Other.

Result: The Specify a device to monitor screen appears.



Specify a device to monitor

Enter the details of the remote unit to monitor.

Connected to: LAN

IP Address: . . .

4 Verify that LAN appears in the Connected to list box.

5 Enter the IP address of the remote unit.

6 Click OK.

Result: The administration Router connects to the remote Router, enabling you to perform remote upgrades, troubleshooting, and so on, as if the telecommuter’s Router were directly connected to your PC.

Establishing the connection over Ethernet

Introduction

This procedure describes how to access a HomeOffice Router to perform remote administration or upgrades or both.

Prerequisites

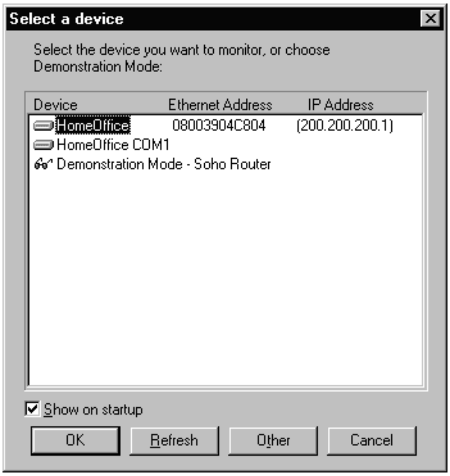
To establish a connection over Ethernet:

- IP connectivity must exist between the PC with Local Manager and the remote HomeOffice Router over the Ethernet interface.
- You need to know the IP address of the remote HomeOffice Router.

To connect to the remote Router over Ethernet

1 On the administration Router, click ▤ (or select Edit > Select device).

Result: The Select a device screen appears.



Select a device

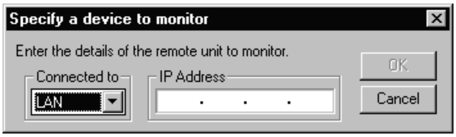
Select the device you want to monitor, or choose Demonstration Mode:

Device	Ethernet Address	IP Address
HomeOffice	08003904C804	(200.200.200.1)
HomeOffice COM1		
Demonstration Mode - Soho Router		

☑ Show on startup

2 Click Other.

Result: The Specify a device to monitor screen appears.



Specify a device to monitor

Enter the details of the remote unit to monitor.

Connected to: LAN

IP Address: . . .

3 Ensure that LAN is shown in the Connected to list box.

4 Enter the IP address of the remote HomeOffice Router.

5 Click OK.

Result: The connection to the HomeOffice Router is established.

Establishing a Telnet connection

Introduction

You can use the Windows Telnet program to access the HomeOffice Router command shell. The procedures given are based on the Telnet program supplied with the version of Windows on your computer.

Note: You only use Telnet access for administrative functions in the command shell. Once connected, you are at the privileged level. When you quit the command shell, the Telnet connection is dropped.

Before you begin

Ensure that your PC is connected to the HomeOffice Router by Ethernet.

To connect to a remote Router with Telnet

1 Start Telnet as follows:

IF you are using	THEN do the following
Windows 3.x	In the Program Manager, select File > Run.
Windows 95 or Windows NT	Click Start > Run.

Result: The Run dialog box appears.

2 Type **telnet** and click OK.

Result: The Telnet program starts.

3 Under the Connect menu, select Remote system.

Result: The Remote System dialog box appears.

4 Set the following parameters:

- Host name: Enter the IP address of the Router to which you want to connect.
- Port: Select telnet.
- TermType: Select vt100.

5 Click Connect.

Result: The system connects you to the command shell. You must enter a password when requested.

6 Enter the password.

Result: The system connects you to the Router in the privileged mode. The prompt that you see is

```
HomeOffice:
```

Section B: Performing upgrades

In this section

Overview

Introduction

Nortel Networks continually works on Meridian HomeOffice II to improve its functionality, and posts product updates on the Nortel Networks web page. You must ensure that the current firmware and software are installed to use new features that have been added.

Obtaining upgrade files

If you must upgrade the firmware or software, you can download the latest upgrade files from the Nortel Networks web site. After you download the upgrade files, you must extract the files contained within them before you can actually perform the upgrades.

Types of upgrades

There are three types of upgrades that you can perform for the HomeOffice Router:

- Install Wizard and Local Manager software upgrade on your PC
- Meridian firmware upgrade
- HomeOffice Router firmware upgrade

The Meridian and HomeOffice Router firmware contain the code necessary for operating the HomeOffice Router. You use the Local Manager software to manage or reconfigure the HomeOffice Router.

Identifying the installed software and firmware release

Introduction

Nortel Networks continually works on Meridian HomeOffice II to improve its functionality, and posts product updates on the Nortel Networks web page. You must ensure that you have current firmware and software to use the new features that have been added.

Note: If you choose not to upgrade the firmware, telecommuters may not be able to use Meridian HomeOffice II if they are

- working in an ACD environment
- using one of the following:
  - — Meridian 2616CT cordless telephone
  - — Meridian 3820 headset
  - — Symposium Communicator card

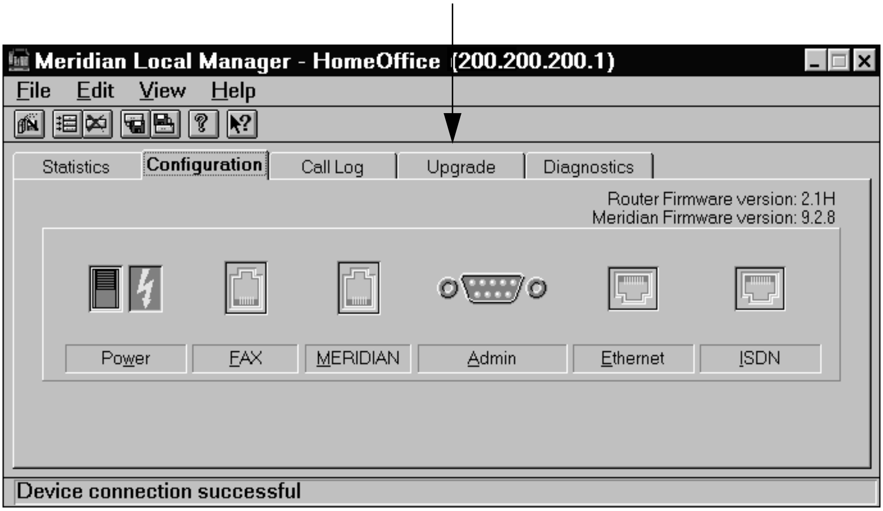
To identify the firmware release you need for these conditions, refer to your *Meridian HomeOffice II Release Notes* (NTP 555-8321-102).

To check the software and firmware versions

1 Start Local Manager.

Result: A screen similar to the following appears.

Click the Upgrade tab

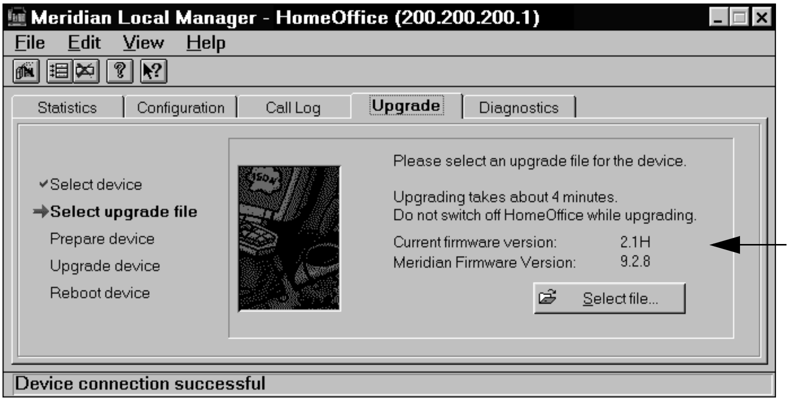


Router Firmware version: 2.1H
Meridian Firmware version: 9.2.8

Device connection successful

2 Click the Upgrade tab.

Result: The Upgrade tab appears, showing the current firmware version.



✓Select device
➜**Select upgrade file**
Prepare device
Upgrade device
Reboot device

Please select an upgrade file for the device.

Upgrading takes about 4 minutes.
Do not switch off HomeOffice while upgrading.

Current firmware version: 2.1H
Meridian Firmware Version: 9.2.8

Device connection successful

Check the firmware version

3 Review the firmware version information on the screen and compare it with the information shown in “To determine if you need to upgrade” on page 365.

Note: There are two types of firmware on your Router:

- motherboard firmware (identified as Current firmware version)
- daughterboard firmware (identified as Meridian Firmware Version)

4 Check the Local Manager software version as follows:

a. Click Help, and then click About Meridian Local Manager.

b. Review the version number on the screen and compare it with the version below.

To determine if you need to upgrade

The following table lists the software and firmware versions when this guide was printed. Check the *Release Notes* on the Nortel Networks web page at http://nortelnetworks.com/homeoffice to obtain more current information.

Component	**Version**
Motherboard firmware	2.1H
Daughterboard firmware	9.2.8
Local Manager and Install Wizard software	2.1H

If the installed software and firmware installed are older than these versions, then you must obtain the latest versions. See “Downloading upgrade files from the Internet” on page 366.

Downloading upgrade files from the Internet

Introduction

If you must upgrade the firmware or software, you can download the latest upgrade files from the Nortel Networks web site. You should download upgrade files into a temporary directory. Once you complete the upgrades, you can delete the download files.

Note: To determine if you need to perform an upgrade, refer to the *Meridian HomeOffice II Release Notes* (NTP 555-8321-102) for the latest information.

Management software

The management software download file is a self-extracting EXE program containing the Install Wizard and Local Manager. After you download the file, you must extract the files contained within it. For instructions, see “Extracting files from the downloaded upgrade files” on page 369.

Firmware

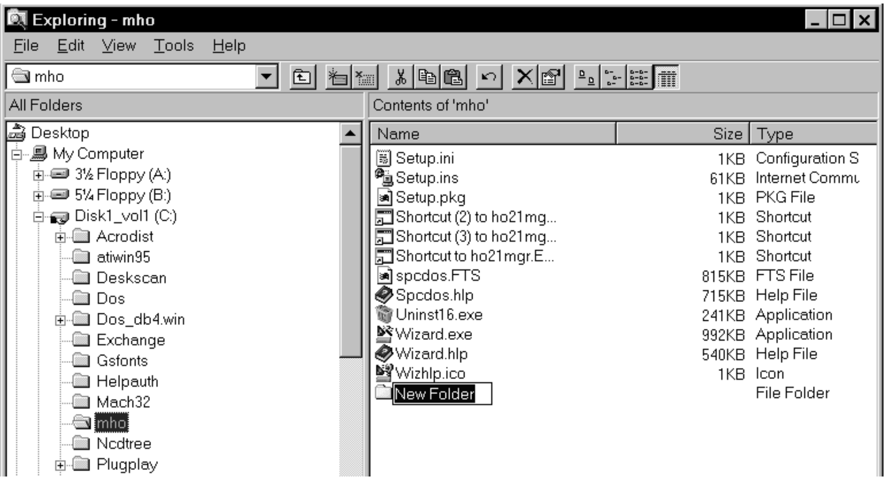
The firmware download file is also a self-extracting EXE program containing firmware for HomeOffice Router hardware. After you download the file, you must extract the files contained within it. For instructions, see “Extracting files from the downloaded upgrade files” on page 369.

To create a temporary folder

1. Open the Program Manager or Windows Explorer.
2. Locate and select the mho directory.

3 Click File > New > Folder.

Result: A NewFolder icon appears in the directory contents column. The New Folder name is selected.



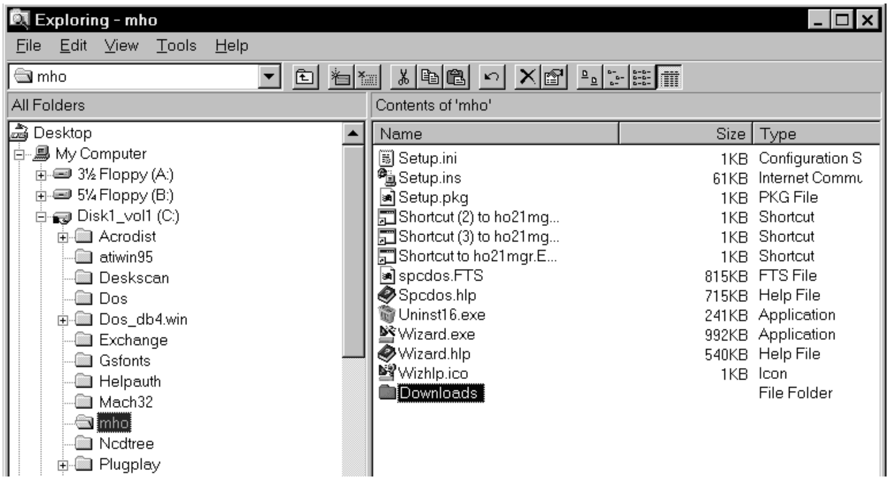
Desktop
- My Computer
  - 3½ Floppy (A:)
  - 5¼ Floppy (B:)
  - Disk1_vol1 (C:)
    - Acrodist
    - atiwin95
    - Deskscan
    - Dos
    - Dos_db4.win
    - Exchange
    - Gsfonts
    - Helpauth
    - Mach32
    - mho
    - Ncdtree
    - Plugplay

Name	Size	Type
Setup.ini	1KB	Configuration S
Setup.ins	61KB	Internet Commu
Setup.pkg	1KB	PKG File
Shortcut (2) to ho21mg...	1KB	Shortcut
Shortcut (3) to ho21mg...	1KB	Shortcut
Shortcut to ho21mgr.E...	1KB	Shortcut
spcdos.FTS	815KB	FTS File
Spcdos.hlp	715KB	Help File
Uninst16.exe	241KB	Application
Wizard.exe	992KB	Application
Wizard.hlp	540KB	Help File
Wizhlp.ico	1KB	Icon
New Folder		File Folder

4 Type a name for the new folder and press Enter.

Note: It is recommended that you name the folder “Downloads.”

Result: The folder is renamed.



Desktop
- My Computer
  - 3½ Floppy (A:)
  - 5¼ Floppy (B:)
  - Disk1_vol1 (C:)
    - Acrodist
    - atiwin95
    - Deskscan
    - Dos
    - Dos_db4.win
    - Exchange
    - Gsfonts
    - Helpauth
    - Mach32
    - mho
    - Ncdtree
    - Plugplay

Name	Size	Type
Setup.ini	1KB	Configuration S
Setup.ins	61KB	Internet Commu
Setup.pkg	1KB	PKG File
Shortcut (2) to ho21mg...	1KB	Shortcut
Shortcut (3) to ho21mg...	1KB	Shortcut
Shortcut to ho21mgr.E...	1KB	Shortcut
spcdos.FTS	815KB	FTS File
Spcdos.hlp	715KB	Help File
Uninst16.exe	241KB	Application
Wizard.exe	992KB	Application
Wizard.hlp	540KB	Help File
Wizhlp.ico	1KB	Icon
Downloads		File Folder

To download the upgrade files

1 With your web browser, connect to the Nortel Networks web site at http://www.nortelnetworks.com/homeoffice.

2 Click Software and Documentation Distribution Center.

3 Locate the software and firmware that you need.

4 Download the file or files into your Downloads folder.

5 Extract the files as described in “Extracting files from the downloaded upgrade files” on page 369.

Extracting files from the downloaded upgrade files

Introduction

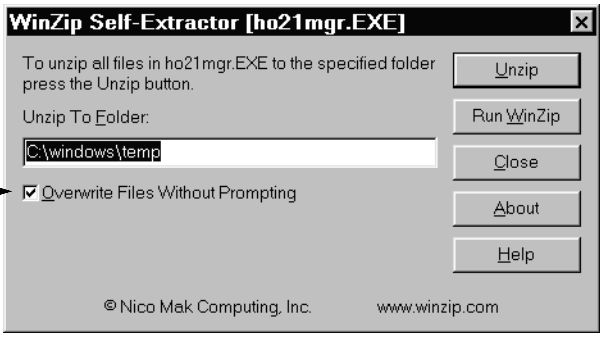
Once you have downloaded the management software and firmware files to your PC, you must extract the files contained within them before you can perform the upgrades.

To perform the extraction using Windows

1 Use Windows Explorer or the Program Manager to navigate to the directory that contains the downloaded upgrade file.

2 Locate and double-click the file that you downloaded.

Result: The WinZip Self-Extractor screen opens.



WinZip Self-Extractor [ho21mgr.EXE]

To unzip all files in ho21mgr.EXE to the specified folder press the Unzip button.

Unzip To Folder: C:\windows\temp

☑ Overwrite Files Without Prompting

© Nico Mak Computing, Inc. www.winzip.com

Ensure this check box is checked.

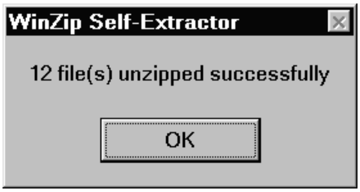
3 Review the information presented and make changes as necessary. (Ensure the Overwrite Files Without Prompting check box is checked.)

Notes:

- It is recommended that you extract the files into the mho directory.
- If you specify a directory that does not exist, the WinZip Self-Extractor creates it.

4 Click Unzip.

Result: The file extraction begins. A status bar shows the extraction progress. When completed, a message similar to the following appears.



WinZip Self-Extractor

12 file(s) unzipped successfully

5 Click OK.

Result: The WinZip Self-Extractor screen reappears.

6 Click Close.

To perform the extraction using MS-DOS

1 Open an MS-DOS session as follows:

- In Windows 3.1/3.11, double-click the MS-DOS icon in the Program Manager (usually in the Main Program group).
- In Windows NT or Windows 95, select MS-DOS Prompt from Programs in the Start Menu.

2 Navigate to your download folder.

3 Enter a command that represents the file that you downloaded.

Result: This command extracts the full management or firmware upgrade kit from the .EXE file.

Note: If you have more than one variation of hardware, then it is permissible to have previously downloaded the firmware upgrade for more than one hardware version into the same directory. When you extract management or firmware upgrade kits from the .EXE file, you receive warnings that some files are about to be overwritten.

Understanding firmware file names

Introduction

If your network uses both the HomeOffice Router and its predecessor, the Soho Router, then files for both types likely exist. The file name identifies the product (and, possibly, the firmware) release. The file name extension identifies the type of firmware file.

File name extensions

The following table identifies the file name extensions:

File type	File name extension
Soho Router motherboard firmware	.UPG
HomeOffice Router motherboard firmware	.UPH
HomeOffice Router daughterboard firmware	.RDB

Examples

- SOFW200.UPG contains firmware for Soho Router Release 2.0.
- MHO21.UPH contains Release 2.1 motherboard firmware for the HomeOffice Router.
- RDB928.RDB contains release 9.2.8 daughterboard firmware for the HomeOffice Router.

Upgrading the management software

Introduction

The SETUP.EXE file contains the management software upgrade, which updates both the Install Wizard and Local Manager software.

When to perform the upgrade

You should perform a software upgrade if you have determined that you are using out-of-date software. For instructions on determining if you need to perform an upgrade, see “Identifying the installed software and firmware release” on page 363.

To perform the management software upgrade

1 Use Windows Explorer or the Program Manager to navigate to the directory that contains the upgrade file.

IF you	THEN
downloaded the upgrade file from the World Wide Web, and then performed the file extraction	find and open the folder that contains the files you extracted (c:\mho).
are using the Meridian HomeOffice II CD-ROM	find and open the SOFTWARE directory on the CD-ROM (d:\software).

2 Double-click the SETUP.EXE file.

Result: The management software installation begins.

3 Follow the prompts on the screen.

4 When the installation is complete, reboot your PC.

Using Local Manager to upgrade the firmware

Introduction

As changes to the HomeOffice Router are made, you may need to update its firmware. You can use this procedure for the following types of upgrades of Routers at both your site and remote telecommuter sites:

- HomeOffice Router firmware upgrade

  This type of firmware contains the code necessary for operating the HomeOffice Router.

- Meridian firmware upgrade

  The Meridian firmware provides the communication path between the HomeOffice Router, a digital telephone, and the corporate PBX.

When to perform the upgrade

You should perform a firmware upgrade if you have determined that you are using out-of-date firmware. For instructions on determining if you need to perform an upgrade, see “Identifying the installed software and firmware release” on page 363.

Before you begin

Before you perform a firmware upgrade, do the following:

1. Ensure that your PC and the HomeOffice Router are connected with an Ethernet cable.
2. Perform the management software upgrade. For instructions, see “Upgrading the management software” on page 372.
3. Shut down any TFTP servers that you may have running on your PC.

4. If you are upgrading remote telecommuter Routers, verify the following:

   — The remote telecommuter is not engaged in a voice call. Voice calls in progress are disconnected.

   — The remote Router is powered on and is not being monitored with Local Manager.

To perform the firmware upgrade with Local Manager

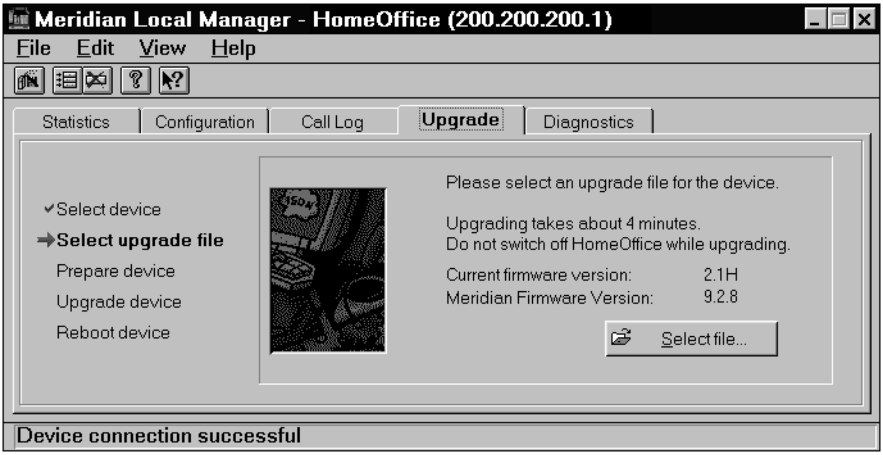
1 Start Local Manager.

2 Select the HomeOffice Router device to upgrade.

Note: For instructions on connecting to a remote telecommuter's Router, see "Establishing a remote LAN-to-LAN connection" on page 355.

3 Click the Upgrade tab.

Result: The Upgrade tab appears, showing the current firmware version.



Please select an upgrade file for the device.

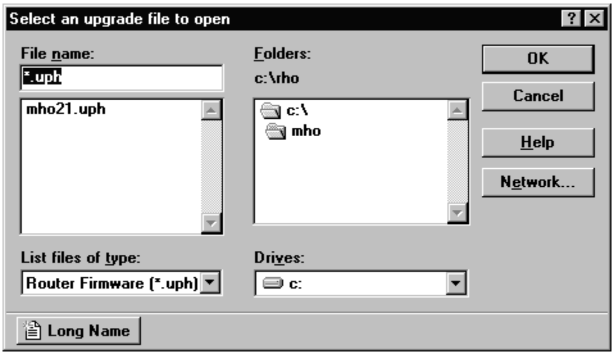
Upgrading takes about 4 minutes.
Do not switch off HomeOffice while upgrading.

Current firmware version: 2.1H
Meridian Firmware Version: 9.2.8

Device connection successful

4 Click Select file.

Result: The Select an upgrade file to open dialog box appears.



Select an upgrade file to open

File name: *.uph

mho21.uph

Folders: c:\rho

c:\
mho

List files of type: Router Firmware (*.uph)

Drives: c:

5 Navigate to the folder containing the upgrade files (for example, c:\mho).

6 Select the file type that you need from the List files of type box:

- Router Firmware (*.uph): These are HomeOffice Router firmware files.
- Meridian phone (*.rdb): These are Meridian firmware files.

Result: All of the files that match the type that you selected are listed in the File name list.

7 Select the file containing the firmware that you want to upgrade and click OK.

Result: The upgrade file now automatically transfers to the HomeOffice Router hardware. Its progress is shown on the screen.

Using the serial port to upgrade firmware

Introduction

This procedure explains how to upgrade the HomeOffice Router firmware using MS-DOS. Use this procedure only if you are unable to upgrade with Local Manager and have been instructed to do so by a technical support representative.

Note: You cannot use this procedure to

- upgrade the Meridian phone firmware (identified by the .RDB file name extension)
- upgrade either the Router or Meridian phone firmware on remote telecommuter Routers (see “Before you begin” below)

This procedure upgrades only the motherboard firmware (identified by file name extension .UPH) on a Router that is locally connected to your PC COM port.

When to perform the upgrade

You should perform a firmware upgrade if you have determined that you are using out-of-date firmware. For instructions on determining if you need to perform an upgrade, see “Identifying the installed software and firmware release” on page 363.

Before you begin

Before you begin the upgrade with the serial port, ensure that the HomeOffice Router ADMIN port is connected to the PC COM port using the RS-232 cable that is supplied with the HomeOffice Router.

To perform the upgrade with the serial port

1. Ensure that the HomeOffice Router is switched off.

2. Connect the RS-232 cable (supplied with the HomeOffice Router) between the ADMIN port on the HomeOffice Router and a free COM port on your PC.

   Make a note of which COM port you used. It is usually COM1 or COM2.

3. Navigate to the directory where the upgrade file is located (for example, c:\mho).

4. With the HomeOffice Router still switched off, start the upgrade by typing **start 1** or **start 2**, where the number is the COM port that you used.

   Result: The upgrade utility checks the validity of the firmware upgrade file. Keep the HomeOffice Router switched off while this happens.

   After a few seconds, the screen background changes to bright blue, and the main upgrade screen appears with the following messages:

   ```
   Please make sure the target unit is powered off.
   Wait for three seconds then switch it on
   Scanning for download target....
   ```

5. Turn on the HomeOffice Router.

   Result: The following message appears:

   ```
   Negotiating link speed
   ```

   After a few seconds, the Link Status line should change to

   ```
   Link established at 115200 baud
   ```

   The upgrade begins and takes a few minutes. You can monitor its progress on the screen.

   When the upgrade is completed, the HomeOffice Router restarts using the new firmware.

6. Close the MSDOS window by typing **exit** (Windows 3.x), or by clicking Close Application.

Section C: Performing other administrative activities

In this section

Overview

Introduction

This section describes some important miscellaneous administration activities.

Tips

With many HomeOffice Routers in your network, daily administration and technical support can be challenging and hectic. This chapter provides some tips to assist administrators and technical support personnel.

Backups and restores

You should store a backup copy of each HomeOffice Router's configuration in the event that remote Router configuration files are corrupted or lost. If you have a backup of the configuration, you can restore it to the Router quite easily.

A configuration backup is also useful when you need to use an alternate configuration.

Reassigning Routers

Periodically, telecommuters leave your organization and new employees are hired to replace them. When this occurs, use the procedure in this section to reassign Routers to replacement employees.

Changing the Meridian password

The Meridian password is a security feature that, unless it is known, prevents telecommuters from making changes to the Local Calls settings (permissions) on the Security tab of the Meridian Circuit Configuration screen. The HomeOffice Router ships with a default password. It is recommended that you change this password and store it in a safe, secure place.

Changing the administration password

If you want to secure the HomeOffice Router's configuration so that telecommuters cannot make configuration changes, you can define a password. The password, if it is not known, prevents a user from making configuration changes using either Local Manager or the command shell.

ATTENTION

Ensure you record the password and store it in a safe secure place. If you forget or lose the password, you must contact your Nortel Networks technical support representative for assistance.

Returning components for repair

If a technical support representative instructs you or a telecommuter to return a HomeOffice Router or digital telephone to Nortel Networks because of a hardware problem, this section provides you with a recommended procedure.

Network maintenance tips

Introduction

This section provides some tips to assist administrators and technical support personnel.

Configuration backup files

Each telecommuter’s HomeOffice Router is an extension of your data network. It is extremely important that you keep a backup copy of each remote telecommuter’s configuration file. If the remote telecommuter’s configuration is corrupted or lost, then you can easily restore it.

If possible, create the backup file using the Config Backup option in Local Manager and store it in a safe, secure location. Ensure that the backup file name easily identifies the telecommuter who owns the file.

For instructions on creating a configuration backup file, refer to the *Meridian HomeOffice II User Guide* (NTP 555-8321-205).

Configuration text files

If you are unable to store backup configuration files, then capture the configuration to a text file. Then either store the text file in soft copy or printed format in a safe, secure location.

For instructions, see “To create a configuration text file” on page 383.

Note: If you use this method and need to restore a configuration, you must manually reconfigure the HomeOffice Router using the information from the text file.

Reference information

Keep hard copies of the Meridian HomeOffice II documentation within easy reach. If this is not possible, provide Adobe Acrobat Reader versions (PDF) of the documentation to each administrator or technical support representative. You can download the documentation from the Nortel Networks web site at http://www.nortelnetworks.com/homeoffice.

Distribute the following information to each administrator and technical support representative:

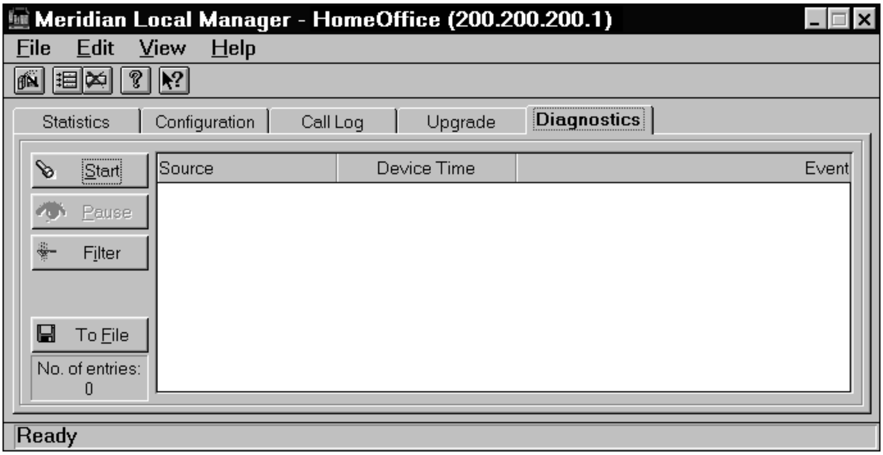
- the “ISDN cause codes” section from the appendixes at the back of the *Meridian HomeOffice II User Guide* (NTP 555-8321-205)
- the Critical and non-critical warnings sections starting on page 404 of this guide

To create a configuration text file

1 Start Local Manager.

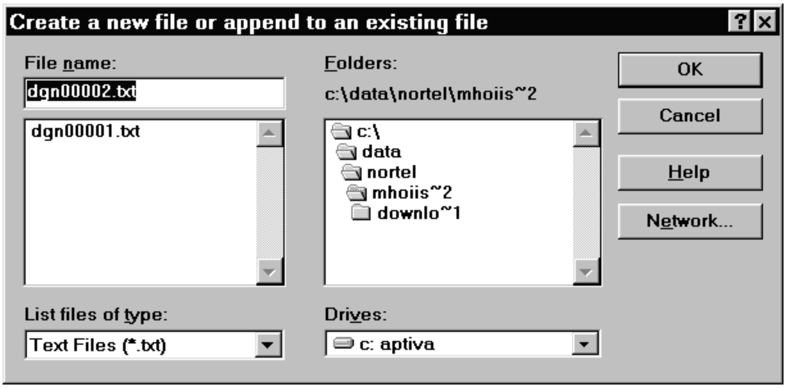
2 Click the Diagnostics tab.

Result: The Diagnostics tab appears.



3 Click To File.

Result: The Create a new file or append to an existing file dialog box appears.



Create a new file or append to an existing file

File name: dgn00002.txt

dgn00001.txt

Folders: c:\data\nortel\mhoiis~2

c:\
data
nortel
mhoiis~2
downlo~1

List files of type: Text Files (*.txt)

Drives: c: aptiva

4 Navigate to the folder where you want to store the file.

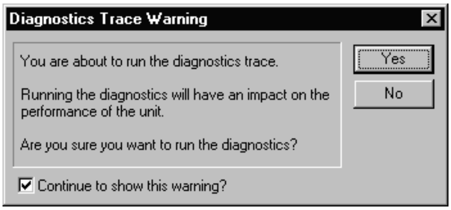
5 Name the file with a name that easily identifies the telecommuter who owns the file.

6 Click OK.

Result: You return to the Diagnostics tab.

7 Click Start to run the diagnostics.

Result: The following warning may appear. Read the warning, and then click Yes.



Diagnostics Trace Warning

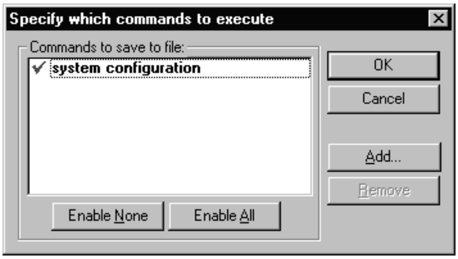
You are about to run the diagnostics trace.

Running the diagnostics will have an impact on the performance of the unit.

Are you sure you want to run the diagnostics?

☑ Continue to show this warning?

The Specify which commands to execute dialog box appears.



Specify which commands to execute

Commands to save to file:

✓ system configuration

8 Ensure that system configuration is selected.

Result: This command captures the Router’s configuration settings into the text file.

9 Click OK.

Result: A series of messages appear indicating that the commands are being processed. When the commands are finished, the messages disappear and you return to the Diagnostics tab.

10 Use any text editor, such as Notepad, to open and view the contents of the text file.

Performing backups and restores

Introduction

This section explains when and why you should back up or restore HomeOffice Router configuration files.

Why create a backup

You should create a configuration backup file for each HomeOffice Router in the network. This way, you have a configuration to go back to if changes that you make to a Router's configuration cause loss of connectivity to the telephone or data networks.

You may also want to create a backup configuration file if you need to connect to more than 14 HomeOffice Routers to perform remote administration, provide technical support, and so on. For more details, see "Administration tips" on page 124.

When to create a backup

Create a backup each time that you make changes to a HomeOffice Router's configuration. Before creating a backup, verify that the connections to the telephone and data network are working correctly.

Note: You can only perform a configuration backup if you are connected to the HomeOffice Router by Ethernet.

When and why you should restore a configuration file

You may want to restore a configuration file if

- you determine that the changes that you made to the configuration caused the telephone or data connection to the corporate network to stop working

- you want to use an alternate configuration

CAUTION

Risk of configuration loss

When you restore a configuration to the HomeOffice Router, it clears any existing settings. If you have any doubts about whether you want to replace the existing configuration, save the configuration to another file by using Config Backup.

Note: You can only perform a configuration restore if you are connected to the HomeOffice Router by Ethernet.

A note about ISDN settings

The following ISDN interface settings are not saved in a configuration backup file. Therefore, each time that you restore a configuration file, you may need to manually configure them in Local Manager:

- Switch Type
- Power Detect

To perform backups and restores

For instructions on performing backups and restores, refer to the *Meridian HomeOffice II User Guide* (NTP 555-8321-205).

Reassigning a HomeOffice Router to another user

Introduction

Periodically, telecommuters leave your organization and new employees are hired to replace them. In cases such as this, you may need to reconfigure and reassign the HomeOffice Router.

To reassign the HomeOffice Router

1. Obtain the previous telecommuter’s Meridian HomeOffice II system.
2. Arrange for configuration changes (additions and deletions) on the Meridian 1 or SL-100 PBX.

   If the HomeOffice II Line Card port is configured with no security, ensure that the configuration for the previous telecommuter is removed or reconfigured to prevent unauthorized use.

   Note: To access the HomeOffice II Line Card port on which security is configured, a hacker must be using a HomeOffice Router that is

   - using the remote ISDN number assigned to that port
   - configured with the security identifier assigned to that port (if used)
3. Arrange for configuration changes (additions and deletions) on the data network.
4. Reconfigure the HomeOffice Router.

   Notes:

   - Ensure that the local calling permissions are reconfigured as required.
   - Ensure that the Meridian password is changed, if required.
5. Provide the new telecommuter with the Meridian HomeOffice II system and the information needed to install and, if required, to configure it.

Changing the Meridian password

Introduction

The Meridian password is a security feature that, unless it is known, prevents telecommuters from making changes to the Local Calls settings (permissions) on the Security tab of the Meridian Circuit Configuration screen. When the HomeOffice Router ships, the default password is *homeoffice*. It is recommended that you change this password and store it in a safe, secure place.

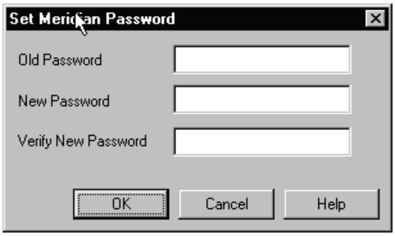
To change the Meridian password

1 Click the Configuration tab.

2 Click the MERIDIAN icon.

3 Select Set Meridian Password from the pop-up menu.

Result: The Set Meridian Password dialog box appears.



4 Enter the current password in the Old Password field.

Result: A series of asterisks (*) appear as you enter the password. This prevents others who may be watching from learning the password.

5 Enter the new password in the New Password field.

Result: A series of asterisks (*) appear as you enter the password.

6 Verify the new password by entering the new password again.

Result: A series of asterisks (*) appear as you enter the password.

7 Click OK.

Result: The Set Meridian Password dialog box closes.

Changing the administration password

Introduction

If you want to secure the HomeOffice Router's configuration so that telecommuters cannot make configuration changes, you can configure the administration password. The password, if it is not known, prevents a user from establishing a connection between Local Manager or the command shell and the HomeOffice Router. This subsequently prevents the user from

- making any configuration changes
- monitoring the HomeOffice Router's status

You should carefully consider whether to secure the configuration with a password. Once the password is defined, you cannot establish a Local Manager or command shell connection without the correct password.

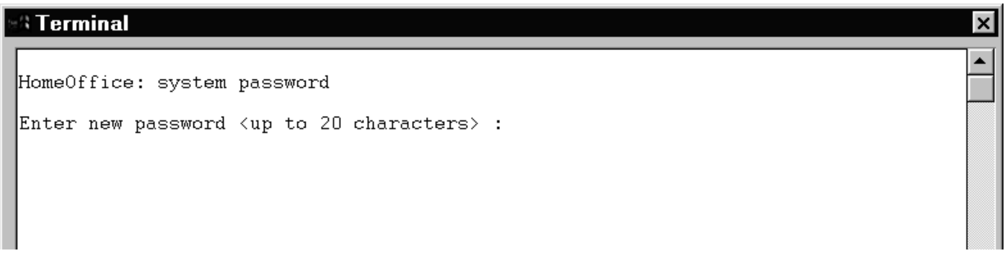
ATTENTION

Ensure that you record the password and store it in a safe secure place. If you forget or lose the password, you must contact your Nortel Networks technical support representative for assistance.

To define the administration password

1. Start Local Manager.
2. On the the Configuration tab, click the Admin icon.
3. Select Set Password from the pop-up menu that appears.

   Result: The Terminal window opens at the `system password` prompt.



```
HomeOffice: system password

Enter new password <up to 20 characters> :
```

4 Type the password (up to 20 characters) and then press Enter.

Note: The cursor does not move or show any characters as you type the password.

Result: The following prompt appears:

```
Re-enter password (up to 20 characters):
```

5 Type the password again and then press Enter.

Result: A message appears indicating whether the password change was successful.

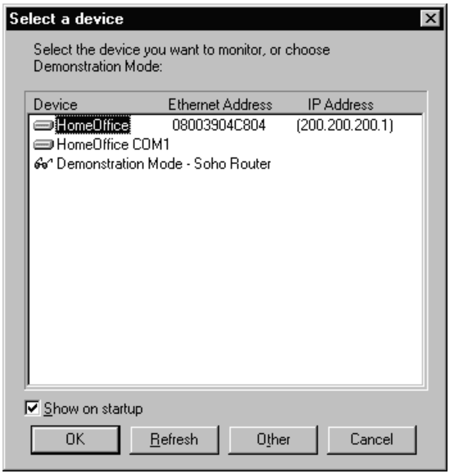
6 Do the following:

IF the password change	THEN
was successful	the following message appears: `Password updated.` Click Close to return to Local Manager.
was not successful	the following message appears: `Password not updated.` At the `Homeoffice: system` prompt, do the following: 1 Type **password** and then press Enter. **Result:** The system prompteds you to enter the password. 2 Repeat steps 4 through 5.

To use Local Manager with the administration password

1 Start Local Manager.

Result: You are prompted to select a HomeOffice Router from the device selection dialog.



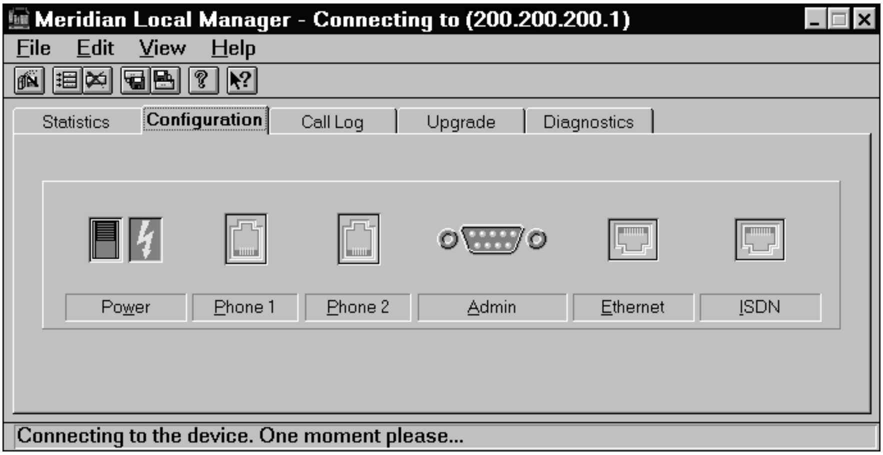
Select the device you want to monitor, or choose Demonstration Mode:

Device	Ethernet Address	IP Address
HomeOffice	08003904C804	(200.200.200.1)
HomeOffice COM1		
Demonstration Mode - Soho Router		

☑ Show on startup

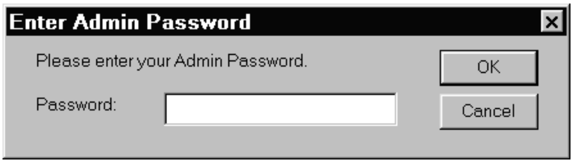
2 Select the device to which you want to connect and click OK.

Result: A window similar to the following appears.



Connecting to the device. One moment please...

After a few seconds, the following dialog appears.



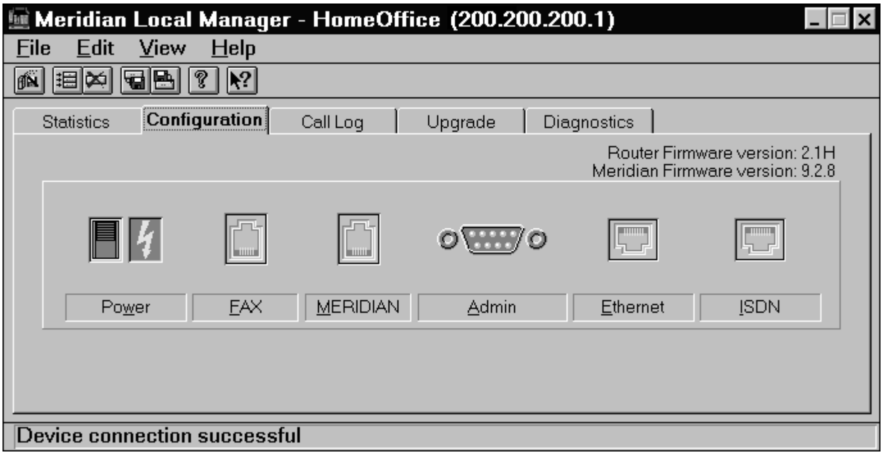
Enter Admin Password

Please enter your Admin Password.

Password:

3 Type the administration password, and then click OK.

Result: The password is verified and if correct, you are connected to the HomeOffice Router.

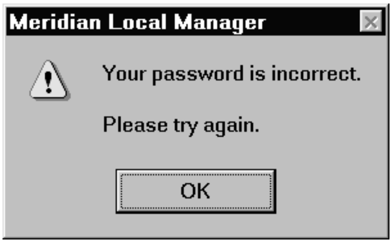


Meridian Local Manager - HomeOffice (200.200.200.1)

Router Firmware version: 2.1H
Meridian Firmware version: 9.2.8

Device connection successful

If the password is not correct, the following dialog appears:



Meridian Local Manager

Your password is incorrect.

Please try again.

If you unable to establish the connection because of a wrong password, contact your technical support representative.

Returning hardware components for repair

Introduction

A technical support representative may instruct you or a telecommuter to return a HomeOffice Router or digital telephone to Nortel Networks because of a hardware problem.

To return the hardware component for repair

1. Obtain the unit (including its cables and accessories) from the telecommuter.
2. Send the unit to the address and contact person that are given to you.
3. Record the return date and any other information that you may need for tracking the status of the return.

   Result: The returned unit is either replaced or repaired and sent back to you.
4. On receipt of the replacement or repaired unit, return it to the telecommuter.

Chapter 5

Troubleshooting network problems

In this chapter

Overview

Introduction

This chapter provides an overview of the items to check if telecommuters are having problems with their Meridian HomeOffice II system. Common symptoms and procedures for performing ISDN and Meridian circuit tests and diagnostics are described in the *Meridian HomeOffice II User Guide* (NTP 555-8321-205).

Component troubleshooting

If telecommuters experience problems with their hardware or are unable to make or receive calls, specific symptoms observed by telecommuters can help you to identify the cause.

The problem can reside on one or more of the following Meridian HomeOffice II components:

- HomeOffice II Line Card on the corporate PBX
- HomeOffice Router hardware or software configuration
- digital telephone
- analog telephone or other analog devices

ISDN or Meridian circuit problems

If telecommuters experience problems with their ISDN or Meridian circuits, you can use the following methods to determine the cause:

- ISDN circuit tests and diagnostics
- Meridian circuit tests and diagnostics

System warnings displayed via command shell

You can also perform troubleshooting by reviewing the system's configuration for warnings.

Use the HomeOffice Router command shell to run the following commands:

- `system configuration`

  This command displays full details on the configuration of the unit and checks for any warnings. If there are outstanding warnings, you must rerun one of the installation commands to correct the problem or problems.

- `system warnings`

  This command displays a list of all warnings.

HomeOffice II component problems

Introduction

If telecommuters experience problems with their hardware or are unable to make or receive calls, specific symptoms observed by telecommuters can help you to identify the cause.

The problem can reside on one or more of the following Meridian HomeOffice II components:

- HomeOffice II Line Card on the corporate PBX
- HomeOffice Router hardware or software configuration
- digital telephone
- analog telephone or other analog devices

HomeOffice Router

The LEDs on the front panel are indications of whether the HomeOffice Router is working correctly. If the LEDs do not display as described in the *User Guide*, there can be

- a problem with the hardware or cabling
- a problem with the ISDN service

Telephones and other analog devices

One or more of the following factors can cause an error message to appear on the digital telephone display, or telecommuters may be unable to make or receive calls:

- The HomeOffice II Line Card port, HomeOffice Router, or both, are configured incorrectly.
- Hardware is faulty, or an unsupported device is being used.
- Cabling connections are completed incorrectly.

Data network connection

Telecommuters may be unable to connect to the data network as a result of

- cabling problems
- faulty hardware (at either the telecommuter's home office or at the corporate office)
- configuration errors on one or more of the following:
  - — telecommuter's HomeOffice Router
  - — telecommuter's Windows PC
  - — remote access switch

More information

For descriptions of component symptoms and what to do about them, refer to the *Meridian HomeOffice II User Guide* (NTP 555-8321-205).

Troubleshooting with Local Manager

Introduction

If telecommuters experience problems with their ISDN or Meridian circuits, you can use the following methods to determine the cause:

- ISDN circuit tests and diagnostics
- Meridian circuit tests and diagnostics

ATTENTION

If you need technical support, capture diagnostic information to a text file before contacting your technical support representative. You may be asked to provide a copy of the diagnostic information for analysis.

Note: Instructions for collecting diagnostics are located in the *Meridian HomeOffice II User Guide* (NTP 555-8321-205).

ISDN loopback, calling, and listening tests

Local Manager provides two types of tests that you can perform on the ISDN interface:

- ISDN loopback test
- ISDN listening and calling tests

The ISDN loopback test verifies HomeOffice Router connectivity. In this test, the HomeOffice Router places a call to itself through the ISDN line and checks that the call can be completed.

ISDN listening and calling tests verify the ability of two devices to connect over ISDN. The tests verify ISDN numbers and check whether the HomeOffice Router supports CLI.

Meridian circuit tests

The two types of tests that you can perform to ensure that the Meridian circuit on the HomeOffice Router is working correctly are

- phone test
- call test

Note: You can also perform a Meridian PBX diagnostic test to collect call progress information for a call to the corporate PBX.

The Meridian phone test ensures that the HomeOffice Router and the digital telephone can communicate with each other.

The Meridian call test ensures that connection to the corporate PBX can be established, verifying that the following are correct:

- directory number used to connect to the PBX
- security identifier used to identify the HomeOffice Router

Diagnostics

You can use the following diagnostics features to determine problem causes:

- ISDN circuit diagnostics
- Meridian circuit diagnostics

The Diagnostics tab in Local Manager allows you to collect, view, and save HomeOffice Router activity as it happens. Use Diagnostics if telecommuters have trouble with ISDN circuits and need information to determine the cause.

If you want to collect progress information for a Meridian circuit call, perform the PBX Diagnostic Test on the Meridian Circuit Configuration screen. The test verifies that the communication path between the HomeOffice Router and the corporate PBX is working by initiating a call to the corporate PBX. It also displays the progress of the ISDN call on the screen, reporting successful connection or an ISDN problem.

You must connect the HomeOffice Router to the digital telephone, and you must configure the Meridian circuit for connection to the corporate PBX.

More information

For instructions on using these tests and diagnostics, refer to the *Meridian HomeOffice II User Guide* (NTP 555-8321-205).

System warnings

Introduction

Another way to perform troubleshooting is to review the system's configuration for warnings.

Using the command shell

Use the HomeOffice Router command shell to run the following commands:

- `system configuration`

  This command displays full details on the configuration of the unit and checks for any warnings. If there are outstanding warnings, you must rerun one of the installation commands to correct the problem or problems.
- `system warnings`

  This command displays a list of all of the warnings.

If you cannot resolve the problem in this way, you may have to reset default values on the HomeOffice Router using the `system reset` command. Once this is done, you must perform the configuration again using one of the installation commands.

Internal warnings

If an internal warning appears, contact your Nortel Networks distributor.

The warning numbers indicate that faults exist. Usually, the lower the number, the more serious the fault. See the following sections for an explanation of critical and non-critical warnings:

- "Critical warnings" on page 404
- "Non-critical warnings" on page 412

Critical warnings

Introduction

The critical warnings listed in the following table indicate that an aspect of the HomeOffice Router configuration could not be applied. Each warning number is associated with a specific fault.

Warning descriptions

Warning number	Fault	Comments
3	IP is disabled	
4	IPX is disabled	
6	Interface is disabled	You see this warning in network <subcontext> circuit tables and in protocol association tables if the interface is disabled.
9	IP is disabled on interface	You see this warning (and warning 10) in protocol association tables if the relevant protocol is disabled on the interface.
10	IPX is disabled on interface	
12	Circuit has not been defined	
13	Circuit is disabled	You see this warning in protocol association tables wherever the network circuit is disabled, either by user selection or incorrect configuration in the network context.
16	IP is disabled on circuit	

Warning number	Fault	Comments
17	IPX is disabled on circuit	
19	Association is inactive	This warning occurs after a restart, indicating a configuration problem not caught by any other warning.
20	Service is inactive	This warning occurs after a restart, indicating a configuration problem not caught by any other warning.
21	Route is inactive	This warning occurs after a restart, indicating a configuration problem not caught by any other warning.
22	Association is on different subnet	You see this warning in the IP protocol association tables. It indicates that an association is incompatible with the subnet mask of the interface. You should change the association address or reorganize your subnet masking.
23	Association has been deactivated	
24	Association address is interface address	You see this warning if your IP or IPX address has been changed to the same address as an association.
25	Reboot required	You see this warning if a configuration change has occurred, requiring a restart of the HomeOffice Router to take effect.
26	Destination is local network	You see this warning if you configure a route to a directly connected IP or IPX network.
27	Next hop is not directly connected	You see this warning if the next hop address is not one of the HomeOffice Router's networks.

Warning number	Fault	Comments
28	Next hop is HomeOffice Router's address	You see this warning if the next hop address of a route is configured to be a local address of the HomeOffice Router.
29	Protocol is incompatible with circuit encapsulation	
30	Circuit is bridging	You see this warning if a circuit configuration is incompatible with a protocol configuration.
31	Circuit is routing	You see this warning if a circuit configuration is incompatible with a protocol configuration.
33	Circuit is not bridging	You see this warning if a circuit configuration is incompatible with a protocol configuration.
34	Circuit is not routing	You see this warning if a circuit configuration is incompatible with a protocol configuration.
36	Interface is not currently routing	You see this warning if a protocol configuration and a circuit configuration clash. you must change either the protocol configuration or the circuit configuration.
37	Interface is not currently bridging	You see this warning if a protocol configuration and a circuit configuration clash. You must change either the protocol configuration or the circuit configuration.
38	Interface is not currently boundary routing	You see this warning if a protocol configuration and a circuit configuration clash. You must change either the protocol configuration or the circuit configuration.

Warning number	Fault	Comments
39	Circuit does not match interface	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
40	Internal: circuit address rejected	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
41	Internal: circuit not registered	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
42	Internal: bad protocol	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
43	Internal: bad secondary circuit	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
44	Internal: circuit has secondary	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.

Warning number	Fault	Comments
45	Internal: duplicate link	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
46	Internal: missing link	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
47	Internal: circuit table full	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
48	Internal: no link	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
49	Internal: no element	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
50	Internal: no memory	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.

Warning number	Fault	Comments
51	Internal: no network	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
52	Internal: no secondary circuit	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
53	Internal: circuit already has a secondary	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
54	Internal: secondary is not a backup	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
55	Internal: circuit closing	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
56	Internal: circuit would not close	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.

Warning number	Fault	Comments
57	Internal: critical circuit change	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
58	Internal: linked circuit is not a primary	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
59	Internal: network type bad	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
60	Internal: circuit using local address	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
61	Internal: invalid encapsulation	You should not see this warning in normal circumstances. If you see one or more of these warnings, contact your technical support representative or your Nortel Networks distributor.
70	Security not enabled for this circuit	Dial-up circuits require the configuration and enabling of the PAP parameters `network <interface> security` command before they can operate. Define PAP ID and peer IDs for all your dial-up circuits. Remember that the remote circuit configuration must be the same as that of the HomeOffice Router.

Warning number	Fault	Comments
71	No primary circuit	You see this warning if you have an orphaned secondary circuit. That is, it has no linked primary circuit. The secondary circuit cannot be used and is disabled.
72	No interfaces configured for bridging	You see this warning in the IP and IPX address tables if you configure the IP and IPX bridge interface addresses when there are no interfaces or circuits currently configured for bridging.
74	No bridge port available	
75	Interface requires PPP encapsulation on bridging circuits	
76	System security key invalid	
77	Chosen authentication not enabled on listener	
78	My identifying name must be entered on listener	
79	Internal: unexpected error	
80	Linked primary is disabled	On a secondary circuit, this indicates that the linked primary circuit is disabled.

Non-critical warnings

Introduction

Non-critical warnings indicate that there is a fault on the HomeOffice Router that may cause erratic behavior, but will not necessarily disable communication entirely.

Each warning number is associated with a specific fault.

Warning descriptions

Warning number	Fault	Comments
81	Linked secondary is disabled	On a primary circuit, this indicates that the linked secondary circuit is disabled.
82	Augmenting with different speed primary interface	For best results, only circuits on interfaces with similar line speeds should be augmented together. This warning indicates that you may have linked a non-optimal pair of circuits.
83	Augmenting with different speed secondary interface	For best results, you should only augment together circuits on interfaces with similar line speeds. This warning indicates that you may have linked a non-optimal pair of circuits.
84	Permanent secondary will always be open	
86	Filtering disabled	
87	Unable to add entry to forwarding database	

Warning number	Fault	Comments
88	Bridge port is disabled	You see this warning in network circuit tables if you have selected bridging, but the corresponding bridge port is disabled. Use the `bridge <interface> enabled` command if this was not intended.
90	SAP disabled on interface	You see this warning in the protocol association tables whenever the relevant protocols have been disabled on a per-interface basis, but are still enabled on a per-circuit basis.
91	RIP disabled on interface	You see this warning in the protocol association tables whenever the relevant protocols have been disabled on a per-interface basis, but are still enabled on a per-circuit basis.
92	SAP disabled because triggered update management disabled	You see this warning if you have selected SAP, but have not chosen triggered update management on the circuit.
93	RIP disabled because triggered update management disabled	You see this warning if you have selected RIP, but have not chosen triggered update management on the circuit.
94	Callback operation set is disabled on this interface	
95	PPP callback Use the `security` command to enable authentication	

Appendix A

Recommended reading

In this appendix

Information available on the Internet

Introduction

You can get more information regarding networking, ISDN BRI, remote access, and other related topics from the web sites listed in this section.

Knowledge bases

http://www.shiva.com/
Click Technical Support to access the Shiva Knowledgebase

http://www.microsoft.com/
Click Support to access the Microsoft Knowledgebase.

http://technet.microsoft.com/
If you subscribe to the Microsoft TechNet, this is an excellent source of information for troubleshooting.

http://www.novell.com/
Click Technical Support to access the Novell Quick Search Knowledgebase.

http://kb.indiana.edu/
Indiana University knowledge base

Networking information

http://www.baynetworks.com/products/Papers/wp-primer.html
Networking: A Primer (a Bay Networks white paper)

http://www.acc.com/internet/about_apu/userprofiles_whitepapers/white_papers/white_papers.html
http://www.acc.com/internet/solutions/white_papers2.html
These Ericsson Inc. sites provide many white papers related to data networking.

http://www.isi.edu/in-notes/iana/assignments/
This site, for technically minded networking experts, provides many reference documents that identify field assignments and parameters for several networking protocols.

http://www.nwconnection.com/
NetWare Connection: The Magazine for Novell® Networking Professionals
Note: Click Past Issues to view the magazine archive.

TCP/IP

http://www.mari.su/techlibrary/win95/faq-c.html
A frequently asked questions (FAQ) list for Windows 95 TCP/IP issues.

http://www.rgb.co.uk/support/guides/tcpip.htm
A TCP/IP white paper.

http://www.cisco.com/cpress/cc/td/cpress/fund/iprf/ip2907.htm
A sample chapter from the following book published by Cisco Press Publications:
IP Routing Fundamentals
Mark Sportack
ISBN: 1-57870-071-X

IPX/SPX

http://www.mari.su/techlibrary/win95/faq-b.html
A frequently asked questions (FAQ) list for Windows 95 IPX/SPX issues.

http://www.isi.edu/in-notes/iana/assignments/novell-sap-numbers
Novell Object Types as used in the Novell Service Advertiser Protocol
Note: You may find this reference document useful for setting up the IPX Service table in Local Manager.

ISDN information

http://www.rgb.co.uk/support/guides/isdn2.htm
ISDN for LAN Internetworking (white paper)

http://www.cnet.com/Content/Reviews/compare/Isdn2/ss05.html
A how-to guide for ordering ISDN service (in the United States)

http://www.cnet.com/Content/Reviews/compare/Isdn2/ss04.html
ISDN: what to look for

http://www.niuf.nist.gov/niuf/docs/443-97/443-97.html
NIUF 443-97 North American ISDN BRI Order Request Form

Remote access information

http://www.rgb.co.uk/support/guides/universl.htm
Understanding Universal Remote Access

http://www.lantronix.com/htmfiles/whitepapers/lrswp.htm
Dial-up Remote Access: Providing flexibility, functionality, and
low cost to your remote connectivity needs (a Lantronix white paper)

Available books

Introduction

You can get more information regarding ISDN and networking from the following books.

ISDN information

A Catalog of National ISDN Solutions for Selected NIUF Applications
North American ISDN User Forum

The Basic Book of ISDN (second edition)
Motorola University Press
Addison-Wesley Publishing Company, Inc.
ISBN 0-201-56374-6

Integrated Services Digital Networks: Architecture / Protocols / Standards
Hermann J. Helgert
Addison-Wesley Publishing Company, Inc.
ISBN 0-201-52501-1

ISDN and Broadband ISDN with Frame Relay and ATM
(3rd edition)
William Stallings
Prentice Hall
ISBN 0-03-415475-X

ISDN Concepts, Facilities, and Services, Second Edition
Gary Kessler
McGraw-Hill, 1993 (2/e)
ISBN 0-07-034247-4

ISDN for Dummies
David Angell
IDG Books Worldwide, Inc.
ISBN 1-56884-331-3

ISDN - How to Get a High-Speed Connection to the Internet
Charles Summers and Bryant Dunetz
John Wiley & Sons, Inc.
ISBN 0-471-13326-4

ISDN in Perspective
Fred R. Goldstein
Addison-Wesley Publishing Company, Inc.
ISBN 0-201-50016-7

ISDN Networking Essentials
Ed Tittel and Steve James
AP Professional
ISBN 0-12-691392-7

ISDN Sourcebook
Information Gatekeepers Inc.
214 Harvard Avenue
Boston, Massachusetts 02134

Sensible ISDN Data Applications
Jeffrey Fritz
West Virginia University Press

Networking information

Networking Standards: A guide to OSI, ISDN, LAN, and MAN Standards
William Stallings
Addison-Wesley Publishing Company, Inc.

Remote Access Essentials
Margaret Robbins
AP Professional
ISBN 0-12-691410-9

Understanding Data Communications: From Fundamentals to Networking
(Second Edition)
Gilbert Held
John Wiley & Sons
ISBN 0 471 96820 X

Appendix B

Configuration forms

In this appendix

Meridian HomeOffice II

Page 1 of 1

Package Contents Checklist

Check	Item
□	HomeOffice Router
□	AC power cord
□	Universal power supply
□	RS-232 cable for connection to administration port
□	Unshielded twisted-pair (UTP) crossover (DTE to DTE) cable for connection to Ethernet card in PC **Note:** This cable may be red from end to end, or gray with a 5.08 cm (2 inches) red sleeve at each end.
□	ISDN cable (similar in appearance to a telephone cable)
□	Meridian HomeOffice II CD-ROM
□	*Meridian HomeOffice II User Guide* and *Release Notes*
□	Digital telephone set with user guide and cable
□	Online/LC key cap for digital telephone set in plastic bag
The following forms (or some other method of providing the information) if telecommuters are to perform their own configuration:	
□	Configuration Instructions
□	HomeOffice Router—ISDN Provisioning Information
□	HomeOffice Router—Meridian Interface Information
□	HomeOffice Router—Security Authentication Information
□	HomeOffice Router—IP Routing Information
	and/or
□	HomeOffice Router—IPX Routing Information
	or
□	HomeOffice Router—Bridging Information
□	Windows PC—TCP/IP Network Configuration Information
□	Windows PC—IPX/SPX Network Configuration Information

Note: See “Cables you must supply yourself” on page 11 of the *Meridian HomeOffice II User Guide* (NTP 555-8321-205) for additional information.

Meridian HomeOffice II Configuration Instructions

Page 1 of 2

Network administrator: Complete one copy of pages 1 and 2 for each telecommuter.

1. Configure the following with the Install Wizard (check all that apply):

   □ ISDN information (includes ISDN switch types, directory numbers, and SPIDs)

   □ Meridian information (includes telephone interface, PBX connection, and security information)

   If one or more of the following network routing options are not checked on this form, call the network administrator for assistance.

   □ IP routing (If checked, refer to the “HomeOffice Router—IP Routing Information” forms for details.)

   □ IPX routing (If checked, refer to the “HomeOffice Router—IPX Routing Information” form for details.)

   □ Bridging (If checked, refer to the “HomeOffice Router—Bridging Information” form for details.)

   □ Security authentication (PAP, CHAP, or SPAP) (If checked, refer to the “HomeOffice Router—Security Authentication Information” form for details.)

2. Perform configuration with Local Manager as follows (attach configuration details separately):

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

3. Install and configure the following on your PC:

   □ TCP/IP (Refer to the “Windows PC—TCP/IP Network Configuration Information” form for details.)

   □ IPX address (Refer to the “Windows PC—IPX/SPX Network Configuration Information” form for details.)

4. Refer to Page 2 of this form for additional instructions: □ yes □ no

Meridian HomeOffice II Configuration Instructions

Page 2 of 2

Network administrator: Complete one copy of pages 1 and 2 for each telecommuter.

5. Additional information (additional details or tasks that you must perform, if necessary):

Meridian HomeOffice II

Page 1 of 2

HomeOffice Router—ISDN Provisioning Information

Part A: Get the following information from the network administrator.

Basic requirements (check all that apply):

You require two B-channels, providing both voice and data capability. Both B-channels must be Circuit Switched Voice and Data (CSVD).

□ Multiple Subscriber Numbering (required if no SPIDs are provided)

Note: If you are in North America, this is for AT&T only.

□ Calling Line Identification (CLI)

□ Additional Call Offering (ACO)

Ordering method - North America only (select only one of the following):

□ Capability package □ EZ-ISDN

Package name: ____________________________________

Part B: Get the following information from the ISDN service provider.

Service provider contact name:	Telephone number:

ISDN line type (check one of the following):

□ National ISDN 1 (NI-1)	□ AT&T 5ESS Custom Multipoint	□ 1RT6
□ National ISDN 2 (NI-2)	□ Euro-ISDN	□ Hong Kong/Taiwan
□ AT&T 5ESS Custom Point-to-Point	□ Austel	□ Other

Note 1: If the ISDN line type is National ISDN 1, National ISDN 2, or AT&T 5ESS, your service provider may need additional information.

Note 2: National ISDN 1, AT&T 5ESS Custom Multipoint, and Euro-ISDN are the only line types that support two directory numbers (a requirement for HomeOffice II).

If you selected Other as the ISDN line type, is phantom power supported? □ yes □ no

Meridian HomeOffice II

Page 2 of 2

HomeOffice Router—ISDN Provisioning Information

Part B (continued): Get the following information from the ISDN service provider.

What is the channel data rate? □ 56 Kbps □ 64 Kbps

What are the ISDN telephone numbers?

Note: Only one number is provided for AT&T Custom. Up to 10 numbers can be provided for Euro-ISDN. Up to two numbers can be provided for all of the other ISDN line types.

You require two telephone numbers for HomeOffice II.

Line 1: ______________________________

Line 2: ______________________________

Line 3: ______________________________

Line 4: ______________________________

Line 5: ______________________________

Line 6: ______________________________

Line 7: ______________________________

Line 8: ______________________________

Line 9: ______________________________

Line 10: ______________________________

What are the Service Profile IDs (SPIDs)?

Note: For NI-1 and AT&T 5ESS Custom Multipoint only.

You require two SPIDs for HomeOffice II. If SPIDs are not provided, then you require Multiple Subscriber Numbering (MSN).

Line 1: ________________________________

Line 2: ________________________________

Meridian HomeOffice II

Page 1 of 1

HomeOffice Router—Meridian Interface Information

1. Assign the ISDN directory numbers (get these from the ISDN service provider).

   Digital telephone (MERIDIAN port calls): ____________________

   HomeOffice Router (data calls): ____________________

   Analog telephone (FAX port calls): ____________________

   Note: The data and fax directory numbers must be the same, but they cannot be the same as the digital telephone number.

Get the following information from the network administrator.

2. PBX connection information

   ISDN directory number to PBX: ____________________

   Note: This is the directory number assigned to the data port on the switch. This directory number must be in a format that can be dialed from the home office (that is, a DID number).

   Security level: □ No security is required □ Security is required

   10-digit security code (only if security is required): ____________________

3. Online/LC key

   You must use this function key (Fkey14 is recommended): ____________________

   Note: You cannot use the selected function key for any other PBX feature. If you select a key that is already programmed for another feature, you will lose that feature on your telephone.

4. Local calling permission

   You may enable the FAX port: □ yes □ no

   Outgoing local calls are allowed on

   - Digital telephone □ yes □ no
   - Analog telephone (FAX port) only □ yes □ no

   Password for setting local calling permissions in Local Manager: ____________________

Meridian HomeOffice II

Page 1 of 2

HomeOffice Router—IP Routing Information

Get the following information from the network administrator.

1. Enable Dynamic IP Address Translation (DIAT for IP): □ yes (complete sections 2 and 4) □ no

If DIAT for IP is enabled, the number of computers connected to HomeOffice Router: □ one □ more than one

If DIAT for IP is not enabled, use unnumbered links? □ yes (complete all of the sections on this form) □ no (complete sections 2 and 4)

If unnumbered links are not used, the IP address of the remote interface device at the host network: ____________________

Note: The address must be on the same network as the ISDN interface (see section 3).

2. Ethernet interface information

HomeOffice Router Ethernet IP address: ____________________

HomeOffice Router Ethernet subnet mask (if not the default): ____________________

IP broadcast style (default is ones): □ ones □ zeros

3. ISDN interface information (complete only if DIAT for IP and unnumbered links *are not* being used)

HomeOffice Router ISDN IP address: ____________________

HomeOffice Router ISDN subnet mask (if not the default): ____________________

4. ISDN circuit information

Name of the remote circuit: ____________________

Primary ISDN telephone number used to call the network site: ____________________

Caller ID (CLID) of the primary ISDN telephone number: ____________________

Secondary telephone number to call the network site (optional required): ____________________

Caller ID (CLID) of the secondary ISDN telephone number: ____________________

Use two B-channels (instead of one)? □ yes □ no

Meridian HomeOffice II

Page 2 of 2

HomeOffice Router—IP Routing Information

5. Will Microsoft Networking be supported? □ yes □ no

   If yes, IP address of the network server: ____________________

6. DHCP information (Configure this in Local Manager if the HomeOffice Router is to function as a DHCP server.)

   Domain name: ____________________

   DNS server IP addresses: ____________________

   ____

   WINS IP addresses: ____________________

   ____

Meridian HomeOffice II

Page 1 of 1

HomeOffice Router—IPX Routing Information

Get the following information from the network administrator.

1. Will Microsoft Networking be supported? □ yes □ no

2. Enable Dynamic IPX Address Translation (DIAT for IPX): □ yes (complete sections 3 and 5) □ no (complete all of the sections on this form)

   If DIAT for IPX is enabled, the number of computers connected to HomeOffice Router: □ one □ more than one

3. IPX Ethernet network information

   IPX network number of HomeOffice Router (8 hex digits): ____________

   IPX frame type: □ SNAP □ 802.2 □ 802.3 □ Ethernet II

4. Complete this section only if DIAT for IPX is not being used.

   Connecting to: □ Intel Shiva LanRover Access Switch □ other device □ do not know

   IPX network number of the ISDN interface: ____________

   Note: You can autogenerate the network number if you are connecting to an Intel Shiva LanRover Access Switch.

   IPX node (MAC) address of the network site (12 hex digits): ____________

   Note: The HomeOffice Router can autodetect the node address of some devices such as the Intel Shiva LanRover Access Switch.

   Use Triggered RIP and SAP? □ yes □ no

5. ISDN circuit information

   Name of the remote circuit: ____________

   ISDN telephone number used to call the network site: ____________

   Second telephone number to call the network site (if required): ____________

   Use two B-channels (instead of one)? □ yes □ no

Meridian HomeOffice II

Page 1 of 1

HomeOffice Router—Bridging Information

Get the following information from the network administrator.

Name of the remote circuit:	
ISDN telephone number used to call the network site:	
Caller ID (CLID) of the network site:	
Second telephone number to call the network site (if required):	
Second Caller ID (CLID) of the network site (if required):	
Use two B-channels (instead of one)?	□ yes □ no
HomeOffice Router IP address (for remote administration or troubleshooting only):	
Subnet mask (if not the default):	

Meridian HomeOffice II

Page 1 of 1

HomeOffice Router—Security Authentication Information

Get the following information from the network administrator.

Type of authentication used: □ PAP □ CHAP □ SPAP □ none

Note: None can be selected if Calling Line Identification is being used.

For PAP, CHAP, and SPAP only:

Your login ID:

Your login password:

Will the network device be able to call the user? □ yes □ no

Complete only if the network device can call the user:

Network device login ID:

Network device login password:

For SPAP only:

User’s ISDN telephone number, if using roaming callback (so the network unit can call the user):

Is additional (third-party) security being used (such as SecurID)? □ yes □ no

User name:

Passcode:

Meridian HomeOffice II

Page 1 of 1

Windows PC—TCP/IP Network Configuration Information

Get the following information from the network administrator.

IP Addresses

IP address assigned or obtained automatically? □ assigned □ obtained automatically

If assigned, the IP address assigned to the PC: ____________________

Subnet mask: ____________________

Gateway IP address: ____________________

Note: The address recorded here is the HomeOffice Router’s Ethernet IP address.

WINS

Obtain WINS server IP addresses from a DHCP server? □ yes □ no

If no, the WINS server IP addresses: ____________________

____

For Windows NT only:

Enable DNS for Windows Resolution? □ yes □ no

Enable LMHOSTS Lookup? □ yes □ no

DNS

Disable DNS? □ yes □ no

If no, the domain name: ____________________

DNS server search order: ____________________

____

Domain suffix search order: ____________________

____

Meridian HomeOffice II

Page 1 of 1

Windows PC—IPX/SPX Network Configuration Information

Get the following information from the network administrator.

Network configuration

Frame type: □ SNAP □ 802.2 □ 802.3 □ Ethernet II

Network number: ______________________

Note: The address recorded here is the HomeOffice Router's Ethernet IPX address.

Logon information (Windows NT only)

Preferred server (if using NetWare 3.x) ______________________

Default tree and context (if using Netware 4.x)

Tree: ______________________

Context: ______________________

Glossary

A

address

A number or string that specifies the destination for data sent across a network.

administrator password

Password used to secure access to a device's configuration.

aggregation

A software method of increasing the effective data capacity of an ISDN connection by combining the capacities of multiple channels of the same type. For example, you can aggregate two 64 Kbps B-channels to act as a single 128 Kbps channel. *See also* bonding.

aging

The process by which a router on an internetwork forgets about networks or devices that are no longer connected. Also called *network aging*.

alert box33

A type of dialog box to which a user can respond simply by clicking a button (such as OK or Cancel), or by pressing Enter or Return.

analog signal

A signal that varies continuously over time, rather than being sent and received in discrete intervals (such as a digital signal). Conventional telephone lines can carry only analog signals, while computers communicate through digital signals.

ASCII (American Standard Code for Information Interchange)

A system used to represent alphanumeric data; a 7-bit-plus-parity character set established by ANSI and used for data communications and data processing. (Pronounced "ASK-ee".)

asynchronous

A method of data communication in which the transmission of data is not synchronized by a clocking signal. Instead, it uses start and stop bits to indicate where characters begin and end in transmitted data packets. The overhead is two extra bits per character transferred. *See also* synchronous.

asynchronous transfer mode (ATM)

An alternative (and more recently developed) networking service. As a cell-based technology, ATM supports voice, video, image, and data applications.

Initial implementations transfer data at 25 to 155 million bits per second, with future data rates approaching 2.5 billion bits per second.

ATM

See asynchronous transfer mode.

augmentation

A networking method of temporarily increasing the data capacity of a channel by combining the capacities of other channels (usually of different types) as needed. For example, an ISDN B-channel can augment the capacity of a leased line to improve performance during peak loads.

authentication

A security technique for authenticating user access to the network, including the user name and password.

authorization

A security technique for authorizing user access to the specific network resources (for example, servers, printers, and databases).

auto-disconnect

A feature automatically releases the connection between a client and a remote access switch when a set number of minutes has elapsed and the unit has not been used. You can control auto-disconnect through either the client or management software, depending on the product.

automatic reconnect

A method of automatically reestablishing the remote connection after an unexpected interruption without user intervention.

B

B-channel

An ISDN bearer channel that carries digitized voice or data at 64 Kbps in either direction. It is a circuit-switched service.

bandwidth

The range of frequencies, from lowest to highest, that a transmission circuit can carry, usually expressed in bits per second (Hz). Bandwidth indicates the maximum transfer rate of a channel.

Basic Rate Interface (BRI)

An ISDN service format for individual users that consists of two bidirectional 64 Kbps bearer channels (or B-channels) that can carry voice or data and one 16 Kbps data channel (D-channel). This combination is often referred to as 2B + D. The data channel can carry low-speed data packets but is generally used to convey call setup and call processing information between the user and the ISDN switch.

baud rate

The rate of the signaling speed of a transmission medium. Once used to indicate the number of bits transmitted each second, bps is now considered to be the more accurate term because each signal can represent more or less than one bit.

bearer channel (B-channel)

The basic unit of channel capacity in a digital telephone network.

bearer rate

The maximum data rate that a switched network connection can support, usually 64 Kbps. Some older network equipment in the United States may limit the bearer rate to 56 Kbps.

bit

A binary unit; the smallest unit of data in the binary counting system. A bit has a value of either 0 or 1.

bits per second (bps)

The basic unit of measure for serial data transmission capacity, which measures how fast data is sent.

bonding

A hardware method of increasing the effective data capacity of a channel by merging the capacities of multiple channels. The network treats a bonded channel as a single connection. The data stream is sliced up into equal portions and each portion is sent over an available circuit. At the receiving end, the data stream is reassembled in the proper order.

BRI

See Basic Rate Interface (BRI).

bridge

A network device that connects two parts of a network located at two different sites so that devices at both sites can communicate.

broadband

A range of bandwidth generally considered to be faster than the T3/E3 range (45/34 Mbps).

broadcast

A network transaction that sends data to all hosts connected to the network.

byte

A group of eight bits, representing one data character.

C

callback

A security feature where a user attempting to connect to a remote networking server is disconnected and then called at a number that has been predefined for that user (in the user document). Also called *dial back*.

central processing unit (CPU)

The computing and control parts of a computer.

channel capacity

The maximum information rate that a channel can support. For example, each ISDN bearer (B) channel has a capacity of 64 Kbps.

CHAP/PAP

Challenge Handshake Authentication Protocol/Password Authentication Protocol. Standard authentication protocols for PPP connections.

character

A standard 8-bit unit representing a symbol, letter, number, or punctuation mark.

circuit switching

A networking method that establishes a dedicated channel between parties for the duration of a call.

clear channel

A channel that places no restrictions on the type of data or data patterns that it can carry. (An example of such restrictions are some digital voice channels that cannot carry long strings of zeros.)

client

An intelligent workstation that makes requests to servers. *See also* server.

client-based application

An application that runs on the client workstation (client) rather than on the server.

client-server architecture

An architecture used on local area networks whereby the server and the individual workstations are treated as intelligent, programmable devices, thus exploiting the full computing power of each.

client software

Multi-protocol PPP client software allowing dial-in access to the public Internet or corporate LANs through a remote access switch or remote access server. The client software dialer establishes and terminates the dial-in connection. The client software PPP driver manages the traffic sent and received across the network link.

COM port

A port on a communications device (such as a router) to which another device (such as a modem) connects. Also, a name commonly used for the RS-232 serial I/O connectors on an IBM PC or other MS-DOS-compatible computer.

command shell

See shell.

compression

The use of special coding to reduce the amount of information being transmitted by eliminating redundancies. With most forms of compression, the information is restored to its original state after transmission. Data compression increases the amount of data that can be carried across WAN connections in a given time. STAC compression can improve ISDN performance by as much as 400%.

configuration file

The file that contains configuration information for a device. *See also* package.

constrained network

A network in which routers are present.

Control Panel

A program that lets users configure some aspect of the operating system environment. Control panels let users change the speaker volume, mouse tracking, color display, network connection software, and so on. You find these programs in the Windows NT or Windows 95 in the Control Panels folder. In Windows 3.x, these programs appear in the Control Panel program (CONTROL.EXE).

CPU

See central processing unit.

D

data channel (D-channel)

An ISDN out-of-band data channel that is used by a terminal and an ISDN switch to exchange control messages that set up and tear down calls on associated bearer channels. It is also used to invoke supplementary services. You can also use the D-channel to communicate low-speed (9600 bps) packet data.

data transfer speed

The speed in bits per second (bps) that data is transmitted across the network.

datagram

A packet of data passed across a network using a connectionless protocol.

Delta technology

Specialized remote adaptive routing protocols for optimizing bandwidth. It prevents unnecessary traffic from being sent over slow WAN connections by sending only the changes (deltas).

device

A hardware unit such as a PC, Macintosh, router, or remote access switch.

device command shell

See shell.

device filtering

The filtering of NBP reply packets that are passing through a remote access switch port from various devices.

DHCP

See Dynamic Host Configuration Protocol (DHCP).

dial back

A security feature where a user attempting to connect to a remote networking server is disconnected and then called at a number that has been predefined for that user. Also called *call back*.

dial in

A mode for remote users to access information on the public Internet or enterprise LAN.

dial-in banner

An optional pop-up window for dial-in connections. Allows network managers to display information or warning messages when users dial in to remote networks.

dial out

A mode for locally connected LAN users to access shared communications equipment to dial up remote information.

digital signal

A signal sent and received in discrete intervals rather than varying continuously over time (as an analog signal does). Conventional telephone lines can carry only analog signals, while computers communicate through digital signals.

directory number (DN)

When using ISDN, the name for a telephone number or subscriber number.

disk operating system (DOS)

A generic term for an operating system whose primary purpose is to manage files and communication with one or more disk drives. This term commonly refers to the operating systems developed by IBM (PC DOS) and Microsoft (MS-DOS) for running IBM-compatible personal computers. The two versions are essentially identical.

DN

See directory number.

dotted decimal notation

A method of specifying IP addresses where a period separates each network portion of the address, and each network portion of the address is a decimal (for example, 123.45.67.89).

download

The process of transferring a file from a server to a client. For remote access switches, it is the process of copying a package file from a disk to the server.

driver

The system software (such as a dial-in driver) under control of the processor that lets applications talk to hardware devices.

drop-down list

In Microsoft Windows, a menu that appears in a location other than the menu bar and drops down when you click it.

dumb-terminal access

Telnet shell command that allows remote terminals to connect to a LAN host. It provides basic terminal server support over the same modems and phone lines used for remote access.

Dynamic Host Configuration Protocol (DHCP)

A TCP/IP protocol allowing the principal parameters of network devices (including IP addresses) to be configured by central DHCP servers.

dynamic IP addressing

Allows a dial-in client to update a variety of TCP/IP protocol stacks with a dynamically acquired address. It removes the burden of assigning per-user IP addresses and is a solution to the issue of dialing into different subnets.

E

end network

The last network number in a network range of numbers.

Ethernet

A high-speed local area network (LAN) that consists of a cable technology and one or more sets of communication protocols. Developed by the Xerox Corporation, Ethernet is based on the IEEE 802.3 standard and uses the carrier sense multiple access with collision detection (CSMA/CD) method to control access to the transmission medium.

Ethernet address

A 48-bit hardware address associated with an individual Ethernet interface card.

Ethernet card

A card in a remote access switch or PC that routes calls over 10Base5 or 10BaseT Ethernet networks.

F

file server

A workstation that runs file server software to provide LAN users with access to shared disks. Also refers to the software that manages the hard disk and other shared resources.

file sharing

A system that allows users to share files among computers that are linked together on a network. For example, on MS-DOS-compatible computers, Windows for Workgroups allows file sharing with other Windows for Workgroups computers.

file transfer protocol (FTP)

A TCP/IP protocol used to send and receive files.

filtering

See device filtering and zone filtering.

firmware

Programs stored in read-only memory (ROM) in a computer or other device. Firmware is usually installed in the device by its manufacturer and cannot be changed or deleted from the device. For remote access switches, firmware can be updated with special files called package files.

fixed dial-back

Dial-back operation where the remote access switch dials a preconfigured phone number. When a dial-in client with fixed dial-back privileges dials in to the remote access switch, the remote access switch hangs up, looks up the fixed dial-back phone number for that user, and dials the phone number.

frame relay

Packet switching technology designed to statistically multiplex the bursts of data traffic from multiple users over a number of logical channels. It is commonly used to connect LANs over a wide area.

FTP

See file transfer protocol.

full duplex

The simultaneous, independent, two-way transmission of data between communicating devices.

G

gateway

An intelligent device used to connect two or more networks at the upper protocol layers of the Open Systems Interconnection (OSI) reference model. The networks can use different protocols and different physical media. A gateway has its own processor and memory.

H

HDLC

See High Level Data Link Control (HDLC).

header compression and broadcast filtering

Client/Server technique used to reduce the overhead associated with LAN-based protocols. It improves the performance of a dial-in link, thus reducing connection times.

High Level Data Link Control (HDLC)

A bit-oriented protocol for communicating synchronous data over wide area networks.

hop

A measure of distance between networks in an internet. One hop consists of a passage through one router.

host

A device connected to a network. *See also* node.

I

in-band signaling

Signal transmission within a frequency range normally used for information transmission.

initialization

The process of bringing a hardware device or a software system to a known state.

Integrated Services Digital Network (ISDN)

An international standard for a worldwide digital communications network intended to replace all current systems with a completely digital transmission system. This type of network has the potential for much greater speeds than standard modem transmissions. ISDN is capable of transmitting voice, data, audio, and video. *See also* asynchronous transfer mode (ATM).

Intel Shiva LanRover Access Switch

A remote access device that connects to ISDN PRI lines. It allows users to dial in to and out of the corporate LAN from workstations with V.34 analog modems, external ISDN terminal adapters, and internal ISDN BRI cards.

Internet

Any interconnected group of networks; an accepted substitute for the word internetwork. When the term Internet is capitalized, it specifically refers to the worldwide, interconnected group of networks and gateways that use the TCP/IP suite of protocols to communicate.

internet address

The Internet Protocol (IP) address by which you can find a specific network service.

Internet Protocol (IP)

A protocol in the TCP/IP protocol suite that manages the routing of data packets between stations on the same or different networks.

internetwork

A collection of individual networks linked by bridges, routers, and gateways. This word is often shortened to internet.

inverse multiplexing

The capability to combine individual dialed channels across a network into a single, higher-speed data stream. The two general types of inverse multiplexing are load balancing and bonding.

IP

See Internet Protocol (IP).

IP address

A 32-bit address assigned to every host that wants to use TCP/IP to communicate across an internet. The address consists of a network and host field. *See* internet address.

IP address pool

Method of assigning IP addresses to dial-in clients. A remote access switch maintains a number of IP addresses that it can assign to dial-in clients.

IP addressing options

Options for assigning dial-in IP addresses to dial-in remote access users (for example, by user, per port, or DHCP server).

IP broadcast address

The IP address used for transmitting packets to all hosts on a given network.

IP Forwarding

A feature that allows a device to provide IP address assignment for dial-in clients.

IP gateway

A feature that enables it to function as a KIP-compatible Datagram Delivery Protocol-IP gateway and to assign IP addresses to dial-in clients running TCP/IP software.

IP network mask

A number that describes both the portion of the device's IP address that represents the network address and the portion of the IP address that represents the host address.

IPCP

IP Control Protocol: Protocol for transporting IP traffic over a PPP connection.

IPX/SPX

The acronyms for internetwork packet exchange (IPX) and sequenced packet exchange (SPX), which are NetWare transport protocols from Novell, Inc.

IPXCP

IPX Control Protocol: Protocol for transporting IPX traffic over a PPP connection.

ISDN

See Integrated Services Digital Network.

ISDN BRI Bonding

ISDN Basic Rate Interface Bonding: Offers the ability to bond two 64 Kbps channels to provide transfer rates up to 128 Kbps.

ISDN BRI Interface

ISDN Basic Rate Interface: Offers support for two 64 Kbps B-channels and one D-channel.

ISDN PRI

ISDN Primary Rate Interface offers support for multiple 64 Kbps B-channels and one D-channel. It is a North American and Japanese 1.544 Mbps ISDN access method comprising 23 (64 Kbps) B-channels and one (64 Kbps) D-channel (23B+D), or an international 2.048 Mbps ISDN access method comprising 30 (64 Kbps) B-channels, one (64 Kbps) D-channel (30B+D), and one (64 Kbps) channel used by the carrier.

K

KIP

The Kinetics Internet Protocol (KIP) gateway software that was developed at Stanford University.

L

LAN

See local area network.

LAN-to-LAN

A function that enables a connection between two or more local area networks (LANs).

launch

Running a computer program or application. *See also* run.

light-emitting diode (LED)

A unit that accepts electrical impulses and converts them into a light signal.

load

To place a program in memory, where it stays resident after it finishes its task, until it is explicitly removed or until the computer is turned off or reset. For example, on MS-DOS-compatible computers, a TSR is an example of a program that is loaded into memory.

load balancing

A type of inverse multiplexing where data packets are alternated over all available circuits. At the receiving end, the packets are reassembled in their proper order.

local

A device capable of a network connection using wires only, as opposed to remote, where a communications device is required for a network connection. For example, local devices are those on your immediate network, while remote devices are those on a network to which you must connect through a remote access switch.

local area network (LAN)

A network system confined to a small geographical area that does not use long-distance carriers such as telephone connections. The area is usually limited by the cable length restrictions of the transportation media being used. *See also* wide area network (WAN).

lookup

A request to which all of the network services of a given type respond with their name and internetwork address. For example, a lookup may find all networked printers in the local zone.

loopback

A diagnostic technique of crossing over a transmit circuit to its associated receive circuit at selected points to locate continuity problems.

M

memory-resident program

See terminate-and-stay-resident (TSR) program.

MLP

See multilink protocol.

multicast

A Data Link layer address that refers to a group of nodes.

multilink protocol (MLP)

A protocol used with ISDN to establish a connection over multiple B-channels (through a process called channel aggregation) to increase the bandwidth of the connection. For example, combining two 64 Kbps B-channels results in an effective potential throughput of 128 Kbps for the connection.

multiplexed channel

A point-to-point channel that shares the capacity (time or frequency) of a physical circuit with one or more channels. For example, an ISDN BRI local loop subdivides its 192 Kbps capacity into two 64 Kbps B-channels, one 16 Kbps D-channel, and a 48 Kbps maintenance channel (which the user cannot access).

multi-protocol support

Support for a range of network protocols allows dial-in access to multiple applications simultaneously, regardless of protocol.

N

name server

A host on the IP network that runs a program to translate host names into IP addresses.

National ISDN-1 (NI-1)

A Bellcore-established ISDN standard used by all Regional Bell Operating Companies (RBOCs) to ensure uniformity among telephone company switches.

NBFCP

See NetBios Framing Control Protocol (NBFCP).

net

An accepted substitute for the word *network*.

NetBEUI

See NetBIOS Extended User Interface.

NetBIOS Extended User Interface (NetBEUI)

A LAN Manager protocol that runs on the Session, Transport, and Network layers of the network architecture.

NetBIOS Framing Control Protocol (NBFCP)

A protocol for transporting NetBios traffic over a PPP connection.

NetWare

The network operating system (NOS) from Novell, Inc., which includes a protocol suite that provides network services and utilities.

network

A group of computers and other devices that communicate with one another over the same wire.

network connector

The interface between a network node and the network wire.

network manager or administrator

The person responsible for administering, setting up, and maintaining a network.

network mask

See IP network mask.

network number

The number by which an individual network is identified. The network number makes up the first part of a network service’s internetwork address on an IP network.

network termination 1 (NT-1)

With ISDN, an electronic device that terminates a two-wire local loop and converts it into a four-wire circuit that carries two B-channels and one D-channel (2B+D). An NT 1 also has its own 48 Kbps channel that provides synchronization and framing, and allows the telephone company to test the local loop.

network termination 2 (NT-2)

Network termination type 2 equipment are devices that provide customer site switching, multiplexing, and concentration (PBXs, computers, terminal controllers).

NI-1

See National ISDN-1.

node

A point at which a device is connected to a network. It is often used to refer to the device itself. A node can be a computer, printer, remote access switch, or any other device.

node ID

The number by which an individual node is identified. The node ID makes up the second part of a network service’s internetwork address on an IP network.

Novell VLM

Novell Virtual Loadable Module client architecture uses packet burst technology, so that multiple packets are sent without waiting for packet-by-packet acknowledgments.

NT-1

See network termination 1.

NT-2

See network termination 2.

O

out-of-band signaling

Transmission outside of the frequency range normally used for information transmission.

P

package

A file containing both the code image and hardware driver (VROM) that gets loaded into a hardware device (such as a remote access switch).

packet

A unit of data transmitted on a network. Also called a *block*.

password

A unique set of characters that protects a network or device from unauthorized access to files or services.

PBX (private branch exchange)

A central control unit for a private telephone system.

peer-to-peer

A networking system architecture in which connected workstations use and provide services such as file sharing.

permissions

Levels of security access available to a user granted by a login process (such as for a dial-in connection, file server connection, and so on).

piggybacking

The process of carrying acknowledgments within a data packet to save network bandwidth. A spoofing synchronism mechanism where routing update messages are sent across the link only when the link is open for real data traffic.

point-to-point configuration

An end-to-end circuit connection with no intermediate processing nodes or access points.

Point-to-Point Protocol (PPP)

A standard method for transporting multi-protocol datagrams over point-to-point links, especially for internet access.

pop-up menu

A menu that appears in a location other than the menu bar and pops up when you click something. This is similar in function to a drop-down list in Microsoft Windows.

port

A point of access into a computer or device. It is the electrical interface through which physical access is gained to the computer or device.

power cycling

Turning the power to the device off and then on.

PPP

See Point-to-Point Protocol.

PRI

See primary rate interface.

primary rate interface (PRI)

An ISDN service that provides 23 B or bearer channels, capable of speeds of 64 Kbps, and a D or data channel, also capable of 64 Kbps. The combined capacity of 1.544 Mbps is equivalent to one T1 line.

protocol

A set of rules for exchanging data between communications equipment.

PSDS

See Public Switched Digital Service.

Public Switched Digital Service (PSDS)

Non-ISDN digital network that restricts ISDN data transmission (to 56 Kbps).

R

random access memory (RAM)

Semiconductor-based memory that can be read from and written to by the microprocessor or other hardware devices. This is generally referred to as volatile memory.

rate adaptation

Sometimes called rate adaption. This is a method that allows a 64 Kbps ISDN channel to transfer slower speed synchronous or asynchronous data. It allows a non-ISDN device to operate on the ISDN network. *See also* V.110 and V.120.

read-only memory (ROM)

Semiconductor-based memory that contains instructions or data that you can read but not modify. (Generally, the term ROM often means any read-only device, as in CD-ROM for Compact Disk, Read-Only Memory.)

remote access

A method that allows a user to connect to a remote network using a computer, a modem, and remote access software.

remote access switch

A network device that connects to analog telephone lines or ISDN BRI lines. It allows users to dial in to and out of the corporate LAN from workstations with analog modems, external terminal adapters, and internal ISDN BRI cards.

remote client

A client at a remote location that uses remote access software to dial in to a network.

remote network

A network at a remote location that is accessed from a local network. *See also* local.

remote node

Remote node software allows remote users to dial in to the corporate LAN, and work with applications and data on the LAN as if the users were actually in the office. By dialing in, they become a node on the LAN. Using a PC, MAC, or UNIX workstation, a modem, and a remote access switch, employees can connect from any location in the world that has an analog, switched digital, or wireless connection.

Reverse Address Resolution Protocol (RARP)

A protocol that supplies a low-level address determination scheme by which a device obtains its IP address from a server.

RJ-11

Standard four-wire connector for phone lines.

RJ-45

Standard eight-wire connector for LANs.

roaming dial back

Dial-back operation where the remote access switch dials the phone number from which it received a call. When a dial-in client with roaming dial-back privileges dials in to the remote access switch, the remote access switch hangs up and dials the phone number from which it received the call.

route

The path that network traffic takes to get from a source to a destination.

router

An intelligent device that links networks together to form an internetwork. Routers know how to send data to any node in the internetwork, but also how to isolate each network so that data is never sent unnecessarily. *See* seed router.

Routing Information Protocol (RIP)

A protocol in the TCP/IP protocol suite that allows gateways and hosts to exchange information about routes to various networks.

routing table

A table of information maintained in each router that lists the next router to which data should be forwarded to reach each possible destination network on an internetwork.

run

On IBM-compatible computers, a term that means to activate an executable program. Similar to *launch* on a Macintosh.

S

S reference point

The reference point between ISDN user terminal equipment (for example, TE1 or TA) and network termination equipment (NT2 or NT1).

secret

Some security services use a secret to encrypt and decrypt packets between security servers and remote access switches. Network administrators must configure the secret both on the security server and on the remote access switches. A secret is usually a hexadecimal value.

SecurID

A network access security system developed by Security Dynamics, Inc. (SDI). SecurID sits between the incoming modem and the remote access switch that provides access to the network. When a dial-in client calls in to the network, the user must first enter the correct SecurID information before connecting to the remote access switch.

SDI manufactures two security solutions that are compatible with remote access switches. The first is a multi-port, stand-alone remote access switch that can be inserted between the remote access switch and the modem. The second, Security Dynamics ACE/Server, is a system of server and client software, and SecurID cards. Once enabled, SecurID authentication is used for the following protocols: IP, IPX, NetBEUI, LLC, and ARA.

seed router

A router that provides network configuration information to other routers on the network. *See* router.

serial device

A device that sends and receives data sequentially, one bit at a time.

serial driver

The system software that allows programs to send and receive data through a serial port.

serial port

A connector on the back of a workstation through which data flows to and from a serial device.

serial transmission

The sequential transmission of data over a data circuit.

server

A network device that provides file-sharing services to multiple computers on a network. *See* client-server architecture.

server-based application

An application that runs partially on the server as opposed to running entirely on the remote station and using only data stored on the server.

Service Advertising Protocol (SAP)

A protocol used by Novell NetWare devices to advertise themselves on the network by broadcasting their names, addresses, and current state.

Service Profile Identifier (SPID)

In ISDN, a number used to identify a set of services or feature parameters subscribed to by a terminal. A SPID is used to distinguish among the different characteristics of multiple terminals that share the same ISDN line. A SPID usually consists of a 10-digit directory number plus an optional suffix. It is supplied by many telephone companies when ISDN service is ordered, and must be used in a terminal initialization procedure.

shell

A program that provides direct communication between the user and the operating system. Also called *command shell* and *device command shell.*

Shiva Password Authentication Protocol (SPAP)

A PPP authentication protocol that allows full use of Shiva network device features, this password is a proprietary network security for PPP links. SPAP is used only for communicating with Intel Shiva LanRover Access Switches.

SLIP

Serial Line Internet Protocol. A standard method for IP packets over remote links.

socket

An endpoint for network communication.

socket number

A number by which an individual service within a node is identified. The socket number is part of a network service's internetwork address. There can be several sockets and, therefore, several network services within the same node.

source routing

A means of data transmission by which the node that generates the transmission determines the route that the data follows.

SPAP

See Shiva Password Authentication Protocol.

SPID

See Service Profile Identifier.

spoofing

A technique that allows a network device to assume the housekeeping responsibilities of a remote terminal. This prevents unnecessary network traffic from being sent across a dial-in or LAN-to-LAN connection, and allows a virtual connection to remain suspended whenever actual network access is not required.

S/T interface

In ISDN, the standard interface for BRI connections consisting of separate transmit and receive pairs that carry two B-channels and one D-channel. When an NT2 device (PBX) is used, the S designation refers to the interface between the NT1 and the NT2; the T designation refers to an identical interface between the NT2 and an ISDN terminal. S/T suggests that no NT2 is present.

S/T reference point

In the absence of the NT2, the user-network interface is usually called the S/T reference point.

STAC compression

STAC Electronics' compression algorithm, which offers up to 400% performance improvement for ISDN and analog remote access applications.

startup disk

A disk containing the system files that the computer uses to boot.

subnet mask

The IP network mask. The subnet mask tells which portion of the device's IP address constitutes the network address and which portion constitutes the host address.

Sub-Network Access Protocol (SNAP)

An Ethernet framing type.

switch type variant

The national or vendor-specific code set extension used by the telephone company switching equipment.

synchronous

A method of data communication in which the transmission of data blocks is timed precisely by a clocking signal. Mainframes and minicomputers generally use clock-driven synchronous transmission; smaller computers generally use asynchronous transmission.

T

TCP/IP

A protocol suite developed by the U.S. Department of Defense (DoD) to connect different types of computers on various types of media while providing data correction, security, and reliability. *See also* Transmission Control Protocol and Internet Protocol.

telecommunications

The process of sending and receiving data over telephone lines.

telnet

A method of remote login for TCP/IP networks. Telnet provides virtual terminal services and allows users to access remote nodes.

terminal

In ISDN, user equipment that terminates a data link (L2) signaling connection on the D-channel.

terminal adapter

A device that connects non-ISDN terminals to an ISDN network.

terminal equipment type 1 (TE1)

End-user ISDN devices that utilize ISDN protocols and support ISDN services (for example, ISDN telephones and workstations).

terminal equipment type 2 (TE2)

Non-ISDN-compatible devices, such as analog telephones and personal computers.

Terminal Endpoint Identifier (TEI)

In ISDN, a number that identifies a specific connection endpoint within a service access point.

terminate-and-stay-resident (TSR) program

On IBM-compatible computers, a program that is loaded into memory, where it remains after it finishes its task, until it is explicitly removed or until the computer is turned off or reset. The users can invoke the program again and again with the aid of a hot key or by an application. A TSR program is often referred to as a memory-resident program.

time out

The process by which a network device is unable to make a connection, and which terminates the session.

time server

A host on the IP network that runs the UDP File Server time protocol (as defined in RFC868) to obtain the time.

T-interface

In ISDN, a standard interface used by BRI devices that connect to a PBX. *See also* S/T reference point.

transceiver

A small box, attached to a network cable and connected to a computer or other device, that provides the drive, reception, and collision detection between physical network media, especially on Ethernet networks. A transceiver is sometimes called a Medium Attachment Unit (MAU).

transceiver cable

A cable connecting an Ethernet device to a transceiver, which, in turn, is attached to the Ethernet cable. A transceiver cable is sometimes called an *Attachment Unit Interface (AUI)*.

Transmission Control Protocol (TCP)

A protocol in the TCP/IP protocol suite that organizes packets, manages their transmission, and ensures their accurate delivery to the receiving station.

transparent

Computer operations that take place automatically, performed either by the operating system or the application, without user intervention or awareness.

U

UART

See universal asynchronous receiver transmitter.

UART port

A serial port on a remote access switch that is intended for out-of-band management of the device.

UDP

See User Datagram Protocol.

U-interface

The physical, electrical, and informational format of the two-wire local loop connection that provides Basic Rate Access. It is the standard connection interface for North American ISDN networks. The U-interface is not accessible to users in other countries.

unconstrained network

A network in which a remote access switch is the only router or there are no routers present.

universal asynchronous receiver transmitter (UART)

A computer module that controls a serial communications port on a personal computer. It contains both receiving and transmitting circuits. A UART module can provide reliable throughput speeds of up to 115 Kbps.

User Datagram Protocol (UDP)

A protocol at the transport layer of the Open Systems Interconnection (OSI) model that defines a connectionless datagram service. A connectionless datagram service sends self-contained packets of data that include destination routing information.

user list

A list that contains the profiles (names, passwords, and permissions) of all of the users who can access a remote access switch.

V

V.110

A form of ISDN rate adaptation. V.110 is a fixed-frame-based rate adaptation standard that subdivides the ISDN channel capacity so it can carry one lower speed (sub-rate) data channel. This standard is rarely used in North America.

V.120

An ISDN rate adaptation standard that is popular in North America, V.120 allows one B-channel to carry multiple subrate channels in a succession of statistically multiplexed (variable-length) frames. These frames support error detection and correction procedures.

V.17

A communication specification developed by ITU-T for fax transmission.

V.22

A communication specification developed by ITU-T for data transfer speeds of up to 1200 bps, full duplex.

V.22bis

A communication specification developed by ITU-T for data transfer speeds of up to 2400 bps, full duplex.

V.32

A communication specification developed by ITU-T for data transfer speeds of up to 9600 bps, full duplex.

V.32bis

A communication specification developed by ITU-T for data transfer speeds of up to 14 400 bps, full duplex.

V.34

A communication specification developed by ITU-T for data transfer speeds of up to 28 800 bps, full duplex.

V.42

An error-correcting technique that incorporates the Link Access Protocol (LAP)-M.

V.42bis

A compression technique for use with V.42 (four-to-1 data compression).

V.90

A communication specification developed by ITU-T for data transfer speeds of up to 56 Kbps.

V.FAST

A communication specification based on the proposed V.34 standard. V.FAST was superseded by the late 1994 release of the official V.34 standard by ITU-T.

virtual connection

A communications link that appears to be a direct, physical link between a sender and a receiver although the link can be through many paths. This is a feature of the remote access switch that controls the cost of telecommunications network services by bringing the connection down when the user is not sending or retrieving data for a user-specified time interval.

virtual read-only memory (VROM) file

An executable file that runs on the main CPU in a remote access switch and is stored in VROM. The VROM file contains the software code used to download an image, hardware drivers, and interfaces, and any miscellaneous functionality that can be accessed by the image.

VROM

See virtual read-only memory (VROM) file.

W

WAN

See wide area network.

wide area network (WAN)

A communications network that connects geographically separated areas.

wildcard character

A keyboard character that is used to represent one or many characters. This character is often used as a means of specifying more than one file by name.

Windows 95 Dial In

Dial-in (remote node) access from Windows 95 clients using PPP as transport.

X

X.21

Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for synchronous operation on public data networks. The recommendation defines the physical characteristics and control procedures to set up calls, transfer data, and terminate calls through the network. Switched or leased circuit communication is supported at data rates of up to and beyond 64 Kbps. X.21 is a mix of three protocols: physical, link, and network. The physical link is a 15-pin connector. The electrical specification (V.11) is capable of data rates of 64 Kbps and higher.

Z

zone filtering

In an AppleTalk network, a security and zone management facility that controls access to AppleTalk zones and services in those zones.

Fields index

Index

Meridian HomeOffice II

Network Administration Guide

Toronto Information Products
Nortel Networks
522 University Avenue, 14th Floor
Toronto, Ontario, Canada
M5G 1W7

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

Publication number:	555-8321-310
Product release:	2.1
Document release:	Standard 01.02
Date:	July 1999

Printed in Canada

NORTEL NETWORKS™

How the world shares ideas.