555-8321-910

Meridian

HomeOffice II

Command Shell User Guide

Standard 01.01 Release 2.1 July 1998

NORTEL

NORTHERN TELECOM

Meridian

HomeOffice II

Command Shell User Guide

Document number: 555-8321-910
Document status: Standard 01.01
Product release: Release 2.1
Date of issue: July 1998

Publication history

July 1998

This is the Standard 01.01 issue of the *Command Shell User Guide* for Release 2.1 of Meridian HomeOffice II. The *Command Shell User Guide* explains how to access the HomeOffice Router command shell and how to use it for configuration.

Contents

About this document

What this document contains

This document describes the following for HomeOffice Router Release 2.1:

- how to access the HomeOffice Router command shell by using
  - Local Manager
  - terminal session
  - Telnet session
- how to use the command shell to configure the HomeOffice Router

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 re-released for the same HomeOffice II release.

Application of version and issue in this documentation release

HomeOffice II documentation release 01.02 is assigned to this issue of *Command Shell User Guide* to support HomeOffice II Release 2.1.

Who should read this guide

This guide is intended for the use of HomeOffice II network managers and administrators.

How this guide is organized

This guide is organized into the following chapters.

Accessing the Command Shell

This chapter describes the methods for accessing the command shell.

Shell commands overview

This chapter provides general instructions on

- using the command shell interface
- using non-privileged and privileged mode commands
- using universal and top-level context commands

Bridge context shell commands

This chapter provides instructions on using shell commands to manage the following bridging functions for the router:

- managing bridging filters
- managing Ethernet and ISDN interfaces
- showing bridging statistics
- showing the bridge forwarding table

IP context shell commands

This chapter provides instructions on using shell commands to manage the following IP routing functions for the router:

- configuring general IP parameters
- configuring parameters for Ethernet and ISDN interfaces
- configuring IP filtering

IPX context shell commands

This chapter provides instructions on using shell commands to manage the following IPX routing functions for the router:

- configuring general IP parameters
- configuring parameters for Ethernet and ISDN interfaces

Network context shell commands

This chapter provides instructions on using shell commands to manage the following physical network interfaces for the router:

- configuring WAN links
- managing Ethernet and ISDN interfaces

SNMP context shell commands

This chapter provides instructions on using shell commands to manage the router's SNMP communities, managers, and traps.

System context shell commands

This chapter provides instructions on using shell commands to set up various parameters that affect the functionality of your local display.

Index

The Index provides an alternate method of locating information in this document.

Conventions used in this guide

Command line interfaces

File and directory names, and prompts and responses in a command line interface are shown in the `courier` font.

The key(s) you are asked to press to complete a command are shown in angle brackets.

Example 1

At the command shell prompt, type the following and press <Enter>:

```
network <interface> configure
```

where <interface> is either `eth1` or `isdn2`.

Example 2

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

Graphical user interfaces

Names of menus, buttons, and lists that you choose in a graphical user interface (such as Windows) are shown in bold typeface.

Example

Choose **Save** and then choose **Exit** from the File menu to save your changes.

Accessing the command shell

Each Meridian HomeOffice Router provides a command shell through which you can configure and manage the unit. You can access the command shell in a number of ways:

- using Local Manager
- using a terminal session
- using a Telnet session

Once you are in the command shell, refer to the “Shell commands overview” chapter for further information.

Procedure 1-1
Using Local Manager to access the command shell

As well as providing a graphical user interface for easy monitoring and management of the HomeOffice Router, the Local Manager allows access to the command shell.

Requirements

In order to access the command shell using the Local Manager, the computer must be connected to the HomeOffice Router either through the serial cable or through the Ethernet cable (both supplied with the router).

Action

Step	Action
1	Start Local Manager. *A device selection dialog appears.*
2	In the device selection dialog, select the router you wish to access, and the connection type. For example, the local router through the COM port. *Local Manager opens.*
3	Click the **Configuration** tab.
4	Click the **Power** or **Admin** icons on the Configuration tab. *A menu appears.*

—continued—

Procedure 1-1 (continued)
Using Local Manager to access the command shell

Step	Action

5 Select the option you need.

If you select	Then

SNMP, **IP Filter**, or **Set Password**	*the relevant context of the command shell opens.*
	You may have to enter a password.
	You are connected to the router in the privileged mode. You see one of the following prompts:
	`HomeOffice:snmp`
	`HomeOffice:ip filter`
	`HomeOffice:system`

Add'l Configurations	*the command shell opens at the top of the privileged mode.* *You are connected to the router in the privileged mode. The prompt you see is:* `HomeOffice:`

—end—

Procedure 1-2
Using a terminal session to access the command shell

You can use a terminal program under Windows 3.x or Windows95 to access the HomeOffice Router command shell through a serial connection. This connection is made using the serial cable between a COM port (for example, COM2) on the Windows computer and the admin connector on the router.

The procedures given are based on the terminal program supplied with the version of Windows on your computer.

Requirements

In order to access the command shell using a terminal session, your computer must be connected to the HomeOffice Router through the serial cable (supplied with the router).

Action

Step	Action
	Windows 3.x
1	Run the Windows terminal program.
2	Under the Settings menu, select **Communications**.
3	Set the following parameters: **a.** Bits per second: **9600** **b.** Data bits: **8** **c.** Stop bits: **1** **d.** Parity: **no parity** **e.** Connector: Choose the COM port connected to the router.
4	Press <Enter>. *You are connected to the router in the non-privileged mode. The prompt you see is:* `Command:`

—continued—

Procedure 1-2 (continued)
Using a terminal session to access the command shell

Step	Action
5	If you want to enter the privileged mode, enter `admin` and press <Enter>. *You are prompted for the password.*
6	Enter the password and press <Enter>. *The following prompt appears:* `HomeOffice:`

Windows95

1 Run the Windows95 **HyperTerminal** program.

2 If you have already saved a HomeOffice Router connection configuration, open this connection by selecting **File - Open** and choosing the connection. If you have not saved a HomeOffice Router connection configuration:

a. Select **File** - **New Connection.**

A new connection dialog box appears.

b. Enter a name and choose an icon for the new connection.

c. Click **OK**.

The Phone Number dialog box appears.

d. In the Phone Number dialog **Connect using:** drop-down menu, select the COM port to which your router is connected, for example, **Direct to COM2**.

e. Click **OK**.

The Port Settings dialog box appears.

f. In the Port Settings dialog set the following parameters:

— Bits per second: **9600**

— Data bits: **8**

— Stop bits: **1**

— Parity: **no parity**

—continued—

Procedure 1-2 (continued)
Using a terminal session to access the command shell

Step	Action
	g. Click **OK**. *Your new connection is saved, and you are connected to the router.*
3	Press <Enter>. *You are connected to the router in the non-privileged mode. The prompt you see is:* `Command:`
4	If you want to enter the privileged mode, enter `admin` and press <Enter>. *You are prompted for the password.*
5	Enter the password and press <Enter>. *The following prompt appears:* `HomeOffice:`

—end—

Procedure 1-3
Using a Telnet session to access the command shell

You can use a Telnet program under Windows 3.x or Windows95 to access the HomeOffice Router command shell through a serial connection. This connection is made using Ethernet.

The procedures given are based on the Telnet program supplied with the version of Windows on your computer.

> ***Note:*** Telnet access is used only 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.

Requirements

In order to access the command shell using a Telnet session, the computer must be connected to the HomeOffice Router by Ethernet.

Action

Step	Action
1	Run the Telnet application. At the File Run command prompt, enter `telnet` *The Telnet program starts.*
2	Under the Connect menu, select **Remote system**. *The Remote System dialog box appears.*
3	In the Remote System dialog box, set the following parameters: **a.** Host name: Enter the IP address of the router. **b.** Port: Select **telnet**. **c.** TermType: Select **vt100**.

—continued—

Procedure 1-3 (continued)
Using a Telnet session to access the command shell

Step	Action
4	Click **connect**. *You are connected to the command shell at the privileged level. You must enter a password when requested.*
5	Enter the password. *You are connected to the router in the privileged mode. The prompt you see is:* `HomeOffice:`

—end—

Shell commands overview

Introduction

Meridian HomeOffice Router commands are available in two modes (or levels):

- non-privileged
- privileged

Non-privileged mode

Non-privileged commands are available to all users; you do not require a password. These commands are available as soon as you log on to the router. Use them, for example, to display statistics or to move to the privileged mode.

You can enter non-privileged mode from either the Local Manager or through a terminal session.

Descriptions of non-privileged mode commands begin on page 2-2.

Privileged mode

Privileged commands are accessed using the `admin` command at the initial router prompt, and are used to configure the router. To access privileged commands you must enter a password. The commands you use to configure the router are grouped into contexts and sub-contexts, according to the network and task type.

You can enter privileged mode from either the Local Manager, through a terminal session, or through a Telnet session.

Descriptions of privileged mode commands begin on page 2-9.

Non-privileged mode commands

Non-privileged mode commands are available as soon as the router is powered on. You do not need to enter a password.

When you are in the non-privileged mode, the system prompt is:

```
command:
```

The following commands are described in this section:

Command	Shortcut	Description
admin	a	Enter privileged mode. You must enter a valid password.
fault	f	Report on conditions indicated by the test LED.
help	h	Display a list of available commands.
quit	q	Return the admin line to idle.
statistics	ss	Display throughput information.
status	st	Display information about the status of each interface.

Note: To display a list of non-privileged commands, enter `help`.

Non-privileged mode commands

admin (a)

Command purpose

The `admin` command lets you enter administration mode and configure the router.

Command syntax

The syntax of the `admin` command is as follows:

```
command: admin
```

Using the command

Once you have entered `admin`, the router prompts you for a password. When the router is shipped, the password is `hello`.

We recommend you change the password immediately using the `system password` command; otherwise the router is not secure. Be sure to keep the password in a safe place. Once you enter the correct password, you enter the administration level.

> ***Note:*** You cannot enter administration level (privileged mode) if someone is already administering the router. Only one administrator at a time can have access to the administration level.

Non-privileged mode commands

fault (f)

Command purpose

The `fault` command gives details of start-up problems. It does not take a parameter.

Command syntax

The syntax of the `fault` command is as follows:

```
command: fault
```

Using the command

The test LED on the front panel of the router flashes RED when a fault is detected. In this case, type `fault` to discover the nature of the fault.

Non-privileged mode commands

help (h)

Command purpose

The `help` command displays

- which commands are available in the current, all, and the following contexts
- which options and parameters can be used with a command
- the spelling of a command

Command syntax

The syntax of the `help` command is as follows:

```
command: help
```

Using the command

Refer to the description beginning on page 2-17.

Non-privileged mode commands

quit (q)

Command purpose

The `quit` command sets the command line to idle and exits non-privileged mode.

Command syntax

The syntax of the `quit` command is as follows:

```
command: quit
```

If you wish to re-enter non-privileged mode, press <Enter>.

Note: After you enter `quit`, the screen below the command line is blank.

Non-privileged mode commands

statistics (ss)

Command purpose

The `statistics` command in non-privileged mode displays a summary of throughput information.

Note: This command is also available in most privileged sub-contexts.

Command syntax

The syntax of the `statistics` command is as follows:

```
command: statistics
```

Using the command

Display the throughput statistics by entering

```
statistics
```

The total number of frames and datagrams transmitted and received on each interface similar to the following appears.

```
                    Frames Received
Interface Frames          Octets           Size Bits/sec
eth1      10945 (99.77%) 4740179 (99.96%) 433  3227
isdn2        25 ( 0.22%)    1533  (0.03%)  61     1
Total     10970          4741712

                    Frames Transmitted
Interface Frames          Octets           Size Bits/sec
eth1      1258   (97.21%)  88046  (98.52%)  69   59
isdn2       26   (2.00%)   1296   (1.45%)   49    0
Total     1294            89362

                    Datagram Statistics
Protocol       Received    Forwarded       Transmitted
ip             8602        406             1635
```

Note: There may be a difference between the number of datagrams forwarded and transmitted. This is because the network layer protocol (IP or CLNP) can transmit a packet to a higher layer of the protocol stack, without that packet ever being forwarded across the network to another device.

Non-privileged mode commands

status (st)

Command purpose

The `status` command provides information about the physical state of each interface.

Command syntax

The syntax of the `status` command is as follows:

```
command: status
```

Using the command

Display the interface status by entering

```
status
```

Status information similar to the following appears:

```
Physical Links

Interface Type  Variant State Bandwidth  Duration
1 eth1   Ethernet Auto   up   10000000  103d 4h 59m 1s
2 isdn2  isdn       BRI  down   128000       2h 5m 23s
```

Column	Description
`Interface`	Tells you the name of the interface.
`Type`	Tells you the type of interface.
`Variant`	Tells you which technology the interfaces use.
`State`	Possible states are `up`, `down`, `testing`, and `disabled`.
`Bandwidth`	Tells you the volume of bps an interface can carry.
`Duration`	Refers to the total length of time the interface has been in its current state.

Note: If an ISDN interface is reported as `up`, this does not mean that it is forwarding. It means that software has loaded successfully.

Privileged mode commands

Privileged mode commands are accessed using the `admin` command at the initial `Command:` prompt, and are used to configure the router. To access privileged commands, you must enter a password. The default password is `hello`. Once you have entered privileged mode, the following prompt appears:

```
HomeOffice:
```

> ***Note:*** You should change the password immediately by using the `system password` command.

The commands you use to configure the router are grouped into contexts and sub-contexts. The following table lists the contexts, sub-contexts, command shell prompt for the current context, available commands in each context, and the page number where the command descriptions begin.

Context	Sub-context	System prompt	Available commands
universal	all sub-contexts	`HomeOffice:`	close, connections, help, open, ping, quit, resume
top	not applicable	`HomeOffice:`	boot, fault, statistics, status
bridge	general	`HomeOffice: bridge general`	configure, forward, statistics
	eth1	`HomeOffice: bridge eth1`	configure, enabled, forward, statistics
	isdn2	`HomeOffice: bridge isdn2`	circuit, forward, statistics
	filter	`HomeOffice: bridge filter`	data, destination, enabled, source, statistics
	span	`HomeOffice: bridge span`	configure, enabled, port, reset, status

—continued—

Context	Sub-context	System prompt	Available commands
ip	general	`HomeOffice: ip general`	address, arp, dhcp, enabled, forward, icmp, relay, rip, route, spoof, statistics
	eth1	`HomeOffice: ip eth1`	address, arp, diat, enabled, icmp, relay, rip
	isdn2	`HomeOffice: ip isdn2`	address, association, circuit, diat, enabled, icmp, lookup, rip
	filter	`HomeOffice: ip filter`	attachments, copy, create, display, edit, remove, test
ipx	general	`HomeOffice: ipx general`	address, datalink, enabled, filtersap, forward, rip, route, sap, service, statistics
	eth1	`HomeOffice: ipx eth1`	address, datalink, enabled, rip, sap
	isdn2	`HomeOffice: ipx isdn2`	address, association, circuit, datalink, diat, enabled, lookup, rip, sap
network	general	`HomeOffice: network general`	decode, multilink, ppp
	eth1	`HomeOffice: network eth1`	address, alias, configure, enabled, statistics, status
	isdn2	`HomeOffice: network isdn2`	activate, address, alias, bap, callback, calls, circuit, configure, default, enabled, multilink, ppp, rates, rejects, security, statistics, status, test, timer, tune, vcs
snmp	-	`HomeOffice: snmp`	community, manager, traps, validate
system	-	`HomeOffice: system`	backup, configuration, edit, isdn, more, password, prompt, protocols, reset, restore, save, security, signon, statistics, store, timeout, trace, upgrade, version, warnings
—end—			

Navigating in the privileged mode

Your current level or context/sub-context in the command shell is indicated by the system prompt, as shown in the preceding table. The following table describes how to navigate from one level to another.

If the level you want to enter is	**Then**	**Example**
below your current level	Type the lower-level name and press <Enter>.	You are at the `HomeOffice:` prompt and want to go to `HomeOffice: ipx eth1`. Type `ipx eth1` and press <Enter>.
above your current level but not at the top	Type the upper-level name and press <Enter>.	You are at the `HomeOffice: ipx eth1` prompt and want to go to `HomeOffice: ipx`. Type `ipx` and press <Enter>.
in another context	Type the full context name and press <Enter>.	You are at the `HomeOffice: ipx eth1` prompt and want to go to `HomeOffice: bridge isdn2`. Type `bridge isdn2` and press <Enter>.
the top level, where the prompt is `HomeOffice:`	Type `top` and press <Enter>.	You are at the `HomeOffice: ipx eth1` prompt and want to go to `HomeOffice:`. Type `top` and press <Enter>.
non-privileged mode	Type `quit` and press <Enter>.	You are at the `HomeOffice: bridge isdn2` prompt and want to exit non-privileged mode. Type `quit` and press <Enter>. The prompt is now `command:`.

Entering commands

You can issue commands in the same way as you change levels, as described in the preceding table. That is:

- If the command is valid at your current level, type the command and parameters, if required, and press <Enter>.
  For example, if you are at the `HomeOffice: network general` prompt and want to issue the ppp command, you type `ppp` and press <Enter>.

- If the command is in a different level, type the context name, command, and parameters, if required, and press <Enter>.
  For example, if you are at the `HomeOffice: network general` prompt and want to issue the bridge span status command, you type `bridge span status` and press <Enter>.

Using shortcuts

Each command described in this document is listed under its full name and shortcut or abbreviation. You can use the shortcut instead of typing the full name.

Universal context commands

The following commands are available in all contexts. Most of them involve the opening and management of Telnet connections. You can make up to three Telnet calls to hosts over the network. Used in this way, the router acts like a terminal server.

The following table describes the commands available in all contexts.

Command	Shortcut	Description
close	cl	Closes the current connection, named connection, or all connections.
connections	con	Shows connections, full information on a named connection, or full information on all connections.
help	h or ?	Displays possible commands or help about commands and contexts.
open	o	Opens a Telnet connection with a host.
ping	p	Pings a remote device.
quit	q	Exits to non-privileged level.
resume	res	Resumes the current or named connection.

To display a list of available commands, enter `help`. To exit to non-privileged level, enter `quit`.

> ***Note:*** You need to press <Break> or <Ctrl-C> to switch out of a current session before you can use the following commands: close, connections, open, remote, resume, and send.

Universal context commands

close (cl)

Command purpose

The `close` command closes the current connection, named connection, or all connections.

> ***Note:*** To display a list of connections, use the `connections` command.

Command syntax

The syntax of the `close` command is as follows:

```
close <connection>
```

where `<connection>` is an optional parameter.

The following table describes the parameters.

Parameter	Meaning	Example
(blank)	The current connection is closed.	close
all	All connections are closed. ***Note:*** You cannot use the `close all` command during a remote administration session.	close all
integer	The specified connection is closed.	close 3

Using the command

To close a particular connection, enter `close`, followed by the connections number. For example, `close 3.`

A list of the remaining connections similar to the following appears. An asterisk indicates the current connection:

```
* connection 1 - 90.2.3.4
  connection 2 - 44.5.6.7
```

Universal context commands

connections (con)

Command purpose

The `connections` command displays information about open connections, or full information on a specific connection.

Command syntax

The syntax of the `connections` command is as follows:

```
connections [<parameter>]
```

where `<parameter>` is an optional parameter.

The following table describes the parameters.

Parameter	Meaning	Example
(blank)	The currently open connections are listed.	connections
IP address or integer	Details of the specified connection are listed.	connections 3

Using the command

Displaying details about currently open connections

To display details about currently open connections, enter `connections`.

A list of the open connections similar to the following appears. An asterisk indicates the current connection.

```
Connections open:
* connection 1 - 89.1.2.3
  connection 2 - 34.08.91.2
```

Universal context commands
connections (con) (continued)

Displaying detailed information for a specific connection

To display detailed information about current connections, enter `connections <IP address or connection number>.`

A list of the open connection's details similar to the following appears. An asterisk indicates the current connection.

```
Local admin line : 3 VC Max, 9600 Baud

* connection 1 - 89.1.2.3
Telnet state : data transfer 28 secs
TCP state    : established
Echo mode    : remote
Binary mode  : on
```

Universal context commands

help (h) and help (?)

Command purpose

The `help` command displays

- which commands are available in the current, all, and the following contexts
- which options and parameters can be used with a command
- the spelling of a command

Using the command

Command help

To view the commands available in the current, all, and the following contexts, enter `help.`

Help text similar to the following appears. (This example is from the `top` *context.)*

```
The following commands are available in the top context:

boot  (b) help (h) status (st)
fault (fa) statistics (ss)

The following commands are available in all contexts:

  close        (cl)    open   (o)    quit    (q)
  connections  (con)   ping   (pi)   resume  (res)

Further commands are available in the following contexts:

  system   snmp   network   bridge   ip   ipx
```

Option and parameter help

To view the options and parameters available for a particular command, enter the command followed by `?`. For example, `system configuration ?.`

Help text similar to the following appears:

```
Enter one of the following:
  summary      (s)             <Return>
```

Universal context commands
help (h)(?) (continued)

Command spelling help

If you are unsure of how to spell a command, type the first letter followed by `?`. The possible ways of completing a valid command line appear.

For example, to determine how to spell the command `statistics` in the `top` context, enter `top s?`.

All possible commands in that context beginning with "s" similar to the following appear. (This example is from the `top` *context.)*

```
The following commands are available :
statistics (ss) status (st)
```

Universal context commands

open (o)

Command purpose

The `open` command establishes a connection to a host. The connection is made using the serial cable between a COM port (for example, COM2) on the Windows computer and the admin connector on the router. You can open up to three connections simultaneously.

> ***Note:*** If you enter an IP address, the router assumes a port number of 23 (the default port number for Telnet sessions) unless you specify otherwise.

Command syntax

The syntax of the `open` command is as follows:

```
open <host IP address>
```

> ***Note:*** The IP address can be in decimal or hexadecimal format.

Using the command

To open a connection to a host, enter `open` followed by the IP address of the host. For example, `open 29.84.30.21.`

If the open command is successful, the host's login prompt similar to the following appears:

```
open 29.84.30.21
Break-in character is <Break>
Trying to make connection...
<Open>
RISC/os (Admin3)
login:
```

Universal context commands

ping (p)

Command purpose

The `ping` command sends a specified number of Internet Control Message Protocol (ICMP) Echo Requests and measures the time taken for the destination device to respond to each request. You can ping another router or host to see if your router can make contact.

Command syntax

The syntax of the `ping` command is as follows:

```
ping
```

Using the command

1 To attempt to make contact with another router or host, enter `ping`.

The router prompts for the Internet address of the device to ping.

```
Host <Internet address> :
```

2 Enter the Internet address.

The router prompts for the size of the ICMP requests. The default size is 64 data bytes.

```
Data size in packet <8 - 1472> (64) :
```

3 Enter the data size.

If you want to accept the default, press <Enter>.

The router prompts for the number of ICMP requests to send. The default value is 16.

```
Number of ICMP requests to send <1-1000000000>(16):
```

4 Enter the number of ICMP requests to send.

If you want to accept the default, press <Enter>.

The router prompts for the time between successive pings. The default is 1000 ms.

```
Interping delay <1 - 60000> (1000) :
```

Universal context commands
ping (p) (continued)

5 Enter the time between pings.

If you want to accept the default, press <Enter>.

The response may look similar to the following:

```
Pinging 41.6.9.8: 64 data bytes.
72 bytes from 41.6.9.8: icmp_seq = 1 time =  10 ms
72 bytes from 41.6.9.8: icmp_seq = 2 time =  10 ms
72 bytes from 41.6.9.8: icmp_seq = 3 time =  10 ms
72 bytes from 41.6.9.8: icmp_seq = 4 time =  10 ms
72 bytes from 41.6.9.8: icmp_seq = 5 time =   0 ms
72 bytes from 41.6.9.8: icmp_seq = 6 time =  10 ms
72 bytes from 41.6.9.8: icmp_seq = 7 time =  10 ms
72 bytes from 41.6.9.8: icmp_seq = 8 time =  10 ms
72 bytes from 41.6.9.8: icmp_seq = 9 time =   0 ms
Host 41.6.9.8 replied to all 9 of the 9 pings
```

If the target router or host replied to the pings, this means that you have full connectivity to the host.

Universal context commands

quit (q)

Command purpose

The `quit` command allows you to leave privileged mode or close the session during a remote administration session.

Note: The quit command is also available as a non-privileged command.

Command syntax

The syntax of the `quit` command is as follows:

```
quit
```

Using the command

To exit privileged mode, enter `quit.`

The following message appears as you leave the privileged mode.

```
Exiting privileged mode
command:
```

To re-enter privileged mode, use the `admin` command.

Universal context commands

resume (res)

Command purpose

The `resume` command lets you access a connection that is already open but is not being used. The connection must have been made using the serial cable between a COM port (for example, COM2) on the Windows computer and the admin connector on the router.

> ***Note:*** You cannot use this command during a remote administration session.

Command syntax

The syntax of the `resume` command is as follows:

```
resume [<parameter>]
```

where `<parameter>` is an optional parameter.

The following table describes the parameters.

Parameter	Meaning	Example
(blank)	The current connection is resumed.	resume
IP address or integer	The specified connection is resumed.	resume 3

Using the command

To resume a connection to a specific host, enter `resume` followed by the IP address of the host or the connection number. For example, `resume 63.49.20.01.`

A response similar to the following appears:

```
Connection resumed to 63.49.20.01
```

Top-level context commands

When you are in privileged level (for instance, by entering `admin` in the non-privileged mode), the top-level context commands are available immediately.

In the top-level context, the command prompt is:

```
HomeOffice:
```

The following top-level context commands are described in this section:

Command	Shortcut	Description
boot	b	Restarts the HomeOffice Router.
fault	fa	Reports on conditions indicated by a red TEST light.
statistics	ss	Displays packet throughput information.
status	st	Displays physical interface status.

To display a list of available commands, enter `help`. To exit to non-privileged level, enter `quit`.

Top-level context commands

boot (b)

Command purpose

The `boot` command lets you restart the router's software.

> ***Note:*** You have to wait a few seconds until the router has restarted before it is available for configuration.

Command syntax

The syntax of the `boot` command is:

```
HomeOffice: boot
```

Using the command

1 Restart the router by entering

`boot`

The router prompts you to confirm this action:

```
Do you wish to restart the unit now <YES or NO>  (
no) :
```

2 Enter `yes` to confirm or press <Enter> to cancel.

If you choose to restart, the following message appears:

```
Restarting HomeOffice .....
```

The router performs a short hardware self-test and then loads its software.

Note: If the hardware self-test fails, the TEST light on the front panel of the router slowly flashes red. If this happens, please contact your supplier.

Top-level context commands

fault (fa)

Command purpose

The `fault` command provides details of start-up problems. If the fault light, which is labeled TEST and is situated on the front panel of the router, flashes red, a fault has occurred. Use the `fault` command to discover the nature of the fault.

Note: This command is also available in non-privileged mode.

Command syntax

The syntax of the `fault` command is:

```
HomeOffice: fault
```

Top-level context commands

statistics (ss)

Command purpose

The `statistics` command displays a summary of throughput information.

> ***Note:*** This command is also available in non-privileged mode and most privileged sub-contexts.

Command syntax

The syntax of the `statistics` command is:

```
HomeOffice: statistics
```

Using the command

1 Display the throughput statistics by entering

```
statistics
```

The total number of frames and datagrams transmitted and received on each interface similar to the following appears:

```
                    Frames Received
Interface Frames          Octets           Size Bits/sec
eth1      10945 (99.77%) 4740179 (99.96%) 433  3227
isdn2        25 ( 0.22%)    1533  (0.03%)  61     1
Total     10970          4741712

                    Frames Transmitted
Interface Frames          Octets           Size Bits/sec
eth1      1258   (97.21%)  88046  (98.52%)  69   59
isdn2       26   (2.00%)   1296   (1.45%)   49    0
Total     1294            89362

                    Datagram Statistics
Protocol       Received    Forwarded       Transmitted
ip             8602        406             1635
```

> ***Note:*** The difference between the number of datagrams forwarded and transmitted arises because the network layer protocol (IP, IPX, or CLNP) can transmit a packet to a higher layer of the protocol stack, without that packet ever being forwarded across the network to another device.

Top-level context commands

status (st)

Command purpose

The `status` command provides information about the physical state of each interface.

Note: This command is also available in non-privileged mode.

Command syntax

The syntax of the `status` command is as follows:

```
HomeOffice: status
```

Using the command

Display the interface status by entering

```
status
```

Status information similar to the following appears:

```
Physical Links

Interface Type  Variant State Bandwidth  Duration
1 eth1   Ethernet Auto   up   10000000  103d 4h 59m 1s
2 isdn2  isdn       BRI  down   128000       2h 5m 23s
```

Column	Description
`Interface`	Tells you the name of the interface.
`Type`	Tells you the type of interface.
`Variant`	Tells you which technology the interfaces use.
`State`	Possible states are `up`, `down`, `testing`, and `disabled`.
`Bandwidth`	Tells you the volume of bps an interface can carry.
`Duration`	Refers to the total length of time the interface has been in its current state.

Note: If an ISDN interface is reported as `up`, this does not mean that it is forwarding. It means that software has loaded successfully.

Alphabetical quick reference

This chapter lists all the commands in alphabetical order. Use this quick reference if you cannot remember the contexts in which a particular command is valid.

Command	Shortcut	Context/sub-context	See
activate	ac	network isdn2	page 7-12
address	ad	ip general ip eth1 or isdn2 ipx general ipx eth1 or isdn2 network eth1 or isdn2	page 5-3 page 5-25 page 6-3 page 6-29 page 7-13
admin	a	non-privileged	page 2-3
alias	al	network eth1 or isdn2	page 7-17
arp	ar	ip general ip eth1	page 5-5 page 5-28
association	as	ip isdn2 ipx isdn2	page 5-30 page 6-34
attachments	a	ip filter	page 5-54
backup	b	system	page 9-3
bap	ba	network isdn2	page 7-19
boot	b	top	page 2-25

—continued—

Command	Shortcut	Context/sub-context	See
callback	cb	network isdn2	page 7-21
calls	ca	network isdn2	page 7-22
circuit	ci	bridge isdn2 ip isdn2 ipx isdn2 network isdn2	page 4-9 page 5-34 page 6-38 page 7-24
close	cl	universal	page 2-14
community	com	snmp	page 8-2
configuration	conf	system	page 9-4
configure	conf	bridge general bridge eth1 bridge span network eth1 or isdn2	page 4-3 page 4-11 page 4-36 page 7-38
connections	con	universal	page 2-15
copy	co	ip filter	page 5-56
create	cr	ip filter	page 5-57
data	da	bridge filter	page 4-17
datalink	d	ipx general ipx eth1	page 6-6 page 6-40
decode	d	network general	page 7-3
default	d	network isdn2	page 7-43
destination	de	bridge filter	page 4-27
dhcp	d	ip general	page 5-6
diat	d di	ip eth1 or isdn2 ipx isdn2	page 5-36 page 6-42

—continued—

Command	Shortcut	Context/sub-context	See
display	d	ip filter	page 5-61
edit	e	ip filter system	page 5-62 page 9-5
enabled	e	bridge eth1 bridge filter bridge span ip general ip eth1 or isdn2 ipx general ipx eth1 or isdn2 network eth1 or isdn2	page 4-12 page 4-30 page 4-39 page 5-8 page 5-39 page 6-8 page 6-43 page 7-44
fault	f	non-privileged top	page 2-4 page 2-26
filtersap	fs	ipx general	page 6-9
forward	fo	bridge general bridge eth1 or isdn2 ip general ipx general	page 4-5 page 4-13 page 5-9 page 6-12
help	h or ?	non-privileged universal	page 2-5 page 2-17
icmp	i	ip general ip eth1 or isdn2	page 5-10 page 5-41
isdn	i	system	page 9-6
lookup	l	ip isdn2 ipx isdn2	page 5-43 page 6-45
manager	m	snmp	page 8-5
more	m	system	page 9-9

—continued—

Command	Shortcut	Context/sub-context	See
multilink	m	network general network isdn2	page 7-6 page 7-46
open	o	universal	page 2-19
password	pa	system	page 9-10
ping	p	universal	page 2-20
port	po	bridge span	page 4-40
ppp	pp	network general network isdn2	page 7-8 page 7-49
prompt	prom	system	page 9-11
protocols	prot	system	page 9-12
quit	q	non-privileged universal	page 2-6 page 2-22
rates	rat	network isdn2	page 7-52
rejects	rej	network isdn2	page 7-54
relay	re	ip general ip eth1	page 5-12 page 5-44
remove	r	ip filter	page 5-66
reset	rst	bridge span system	page 4-42 page 9-14
restore	rst	system	page 9-16
resume	res	universal	page 2-23
rip	ri	ip general ip eth1 or isdn2 ipx general ipx eth1 or isdn2	page 5-16 page 5-47 page 6-14 page 6-46

—continued—

Command	Shortcut	Context/sub-context	See
route	ro	ip general ipx general	page 5-19 page 6-15
sap	sa	ipx general ipx eth1 or isdn2	page 6-19 page 6-48
save	sa	system	page 9-17
security	sec se	network isdn2 system	page 7-56 page 9-18
service	ser	ipx general	page 6-20
signon	si	system	page 9-19
source	so	bridge filter	page 4-31
spoof	sp	ip eth1	page 5-51
statistics	ss	non-privileged top bridge general bridge eth1 or isdn2 bridge filter ip general ipx general network eth1 system	page 2-7 page 2-27 page 4-6 page 4-14 page 4-34 page 5-22 page 6-25 page 7-63 page 9-20
status	st	non-privileged top bridge span network eth1 or isdn2	page 2-8 page 2-28 page 4-43 page 7-68
store	st	system	page 9-21
test	te	ip filter network isdn2	page 5-67 page 7-69

—continued—

Command	Shortcut	Context/sub-context	See
timeout	ti	system	page 9-22
timer	ti	network isdn2	page 7-75
trace	tra	system	page 9-23
traps	tra	snmp	page 8-8
tune	tu	network isdn2	page 7-77
upgrade	upg	system	page 9-35
validate	v	snmp	page 8-11
vcs	v	network isdn2	page 7-84
version	v	system	page 9-37
warnings	w	system	page 9-38
—end—			

Bridge context shell commands

Introduction

The `bridge` context manages the router's bridging functions. The commands are grouped into the sub-contexts listed in the following table.

Sub-context	Description
general	Commands for bridging statistics and showing the Bridge forwarding table.
eth1	Commands for managing an Ethernet interface.
isdn2	Commands for managing an ISDN interface.
filter	Commands for managing bridge filtering.
span	Commands for managing the Spanning Tree Algorithm.

Some protocols need to have certain parameters set up separately for each interface. Commands dealing with these parameters are not described in the `bridge general` context, but in the protocol-specific sections. For instance, commands that are available only in the `filter` or `span` sub-contexts are described in the appropriate sections.

Bridge general sub-context commands

In the `bridge general` sub-context, the command prompt is:

```
HomeOffice: bridge general
```

The following `bridge general` sub-context commands are described in this section:

Command	Shortcut	Description
configure	conf	Defines the Bridge forwarding table time-out period.
forward	fo	Displays the Bridge forwarding table for all interfaces.
statistics	ss	Displays bridging statistics for all interfaces.

To display a list of available commands, enter `help`. To quit and return to non-privileged level, enter `quit`.

Bridge general sub-context commands

configure (conf)

Command purpose

In the `bridge general` sub-context, the `configure` command defines the entry time-out period in the Bridge forwarding database for all bridging interfaces.

The Bridge forwarding database stores the addresses of destination hosts and the elapsed time a packet was last received from them. If a host is on the same segment of the network, the corresponding entry is used to localize traffic to it. The time-out value defined with this command is the length of time an entry is stored in the Bridge forwarding table before being discarded.

Command syntax

The syntax of the `configure` command is as follows:

```
HomeOffice: bridge general configure [<show>]
```

where `<show>` is an optional parameter that displays the current Bridge forwarding table entry time-out setting.

If no parameter is provided you are asked to provide a time-out setting.

Using the command

Displaying the current Bridge forwarding table entry time-out setting

Display the current Bridge forwarding table entry time-out setting by entering

```
bridge general configure show
```

A message similar to the following appears:

```
Bridge forwarding table entry timeout in seconds:
200
```

Note: This value applies to all bridging interfaces.

Bridge general sub-context commands
configure (conf) (continued)

Changing the current Bridge forwarding table entry time-out setting

1 Change the current Bridge forwarding table entry time-out setting to 200 seconds by entering

```
bridge general configure
```

The router prompts you for a time-out value. The default is 300 seconds.

```
Bridge forwarding table entry timeout in seconds
<10-1000000> (300):
```

2 Type `200` and press <Enter>.

A confirmation message similar to the following appears:

```
Bridge configuration updated:
Bridge forwarding table entry timeout in seconds:
200
```

Bridge general sub-context commands

forward (fo)

Command purpose

The `forward` command lets you check the entries currently stored in the dynamic forwarding database for all bridging interfaces. The entries are shown separately for each interface.

Command syntax

The syntax of the `forward` command is as follows:

```
HomeOffice: bridge general forward
```

Using the command

To display entries currently stored in the dynamic forwarding database for all bridging interfaces, enter

```
bridge general forward
```

A list of entries similar to the following appears:

```
Bridge Forwarding Table

Port : eth1    Entries : 12
00-00-6B-80-00-72    00-00-6B-80-08-F8    *00-00-6B-81-04-2C
00-00-6B-81-04-4E    00-00-6B-81-09-18    *00-00-6B-81-09-5E
00-00-6B-81-10-EE    00-00-6B-81-21-06     00-00-6B-81-24-26
00-00-6B-81-2C-7C    00-00-6B-81-2C-96     00-00-6B-81-2C-A2
-- MORE --
```

Note: In this example, the first interface shown is `eth1`, for which there are twelve entries.

Bridge general sub-context commands

statistics (ss)

Command purpose

This command displays or resets frame and packet statistics for each bridging interface. The entries are shown for each interface separately.

Command syntax

The syntax of the `statistics` command is as follows:

```
HomeOffice: bridge general statistics
```

Using the command

1 To display or reset frame and packet statistics for each bridging interface, enter

```
bridge general statistics
```

The router prompts you to select either frames or reset (the default is frames).

```
Statistics <FRAMES or RESET> (frames) :
```

If you want to	Then
display frame and packet statistics	go to step 2
reset frame and packet statistics	go to step 3

2 To display frame and packet statistics, select `frames`.

A list of frame and packet statistics for each bridging interface similar to the following appears:

```
Bridge Statistics: eth1

Total frames in             :     878030 (100.00%)
     Forwarded to port      :       5991 (  0.68%)
     Port not forwarding    :       2399 (  0.27%)
     Filtered dynamically   :     869640 ( 99.04%)
     Filtered statically    :          0 (  0.00%)

Total frames out            :          1 (100.00%)
     Forwarded to port      :          0 (  0.00%)
     Port not forwarding    :          1 (100.00%)
     Filtered statically    :          0 (  0.00%)
```

Bridge general sub-context commands
statistics (ss) (continued)

```
Bridge Statistics: isdn2

Total frames in             :          0 (  0.00%)
     Forwarded to port      :          0 (  0.00%)
     Port not forwarding    :          1 (100.00%)
     Filtered dynamically   :          0 (  0.00%)
     Filtered statically    :          0 (  0.00%)

Total frames out            :          1 (100.00%)
     Forwarded to port      :          0 (  0.00%)
     Port not forwarding    :          1 (100.00%)
     Filtered statically    :          0 (  0.00%)
```

Note 1: Forwarded to Port means that the frame has been transmitted out on this interface.

Note 2: Port not forwarding means that the port is not passing bridge traffic. For example, when Spanning Tree has shut it down to prevent a loop.

Note 3: Filtered dynamically means that the frame has been discarded because the router knows the destination is local and therefore the packet does not need to be sent across the WAN.

Note 4: Filtered statically counts the number of frames discarded as a result of a match with a filter configured by the user.

3 To reset frame and packet statistics, select `reset`.

The statistics for each bridging interface are reset, and the following message appears:

```
Bridge statistics have been reset.
```

Bridge interface-specific sub-context commands

The commands in the `bridge eth1` or `isdn2` sub-context let you manage the HomeOffice Router's Ethernet or ISDN interface.

The command prompts are:

```
HomeOffice: bridge eth1
```

```
HomeOffice: bridge isdn2
```

The following table describes the commands in this section:

Command	Shortcut	Interface	Description
circuit	ci	isdn2	Applies to ISDN interface only. Creates a circuit for a remote destination.
configure	conf	eth1	Applies to Ethernet interface only. Configures the priority of Ethernet interface.
enabled	e	eth1	Applies to Ethernet interface only. Enables or disables the bridge port state.
forward	fo	eth1 isdn2	Applies to both interfaces. Displays the Bridge forwarding table for all interfaces.
statistics	ss	eth1 isdn2	Applies to both interfaces. Shows static filtering statistics.

To display a list of available commands, type `help` or access online help. To exit back to non-privileged level, enter `quit`.

CAUTION
Loss of connectivity
Be careful when changing bridge port configurations, especially in remote administration sessions; it is possible to exclude yourself from the unit, and you may need local administration to restore connectivity.

Bridge interface-specific sub-context commands

circuit (ci)

Command purpose

The `circuit` command configures the ISDN interface for bridging.

Command syntax

The syntax of the `circuit` command is as follows:

```
HomeOffice: bridge isdn2 circuit
```

Using the command

1 To configure the ISDN interface for bridging, enter

```
bridge isdn2 circuit
```

The router prompts for the name of the circuit.

```
Circuit Name <Up to 15 Characters or *> :
```

2 Enter the name of the circuit to configure.

The router prompts you to enable the circuit. The default is `enabled`.

```
Bridge port state <ENABLED or DISABLED> (enabled) :
```

3 Enable the bridge port to bridge traffic, if required, by pressing <Enter>. Otherwise type `disabled` to disable the circuit.

Note: You can enable the circuit later.

The router prompts you to add the bridge port path cost. The default is 15625.

```
Bridge port path cost <1 - 65535> (15625) :
```

4 Enter the bridge port path cost (this port's contribution to the Root Path Cost).

The Root Path Cost is the sum of the Path Costs of the bridges between this bridge and the Root Bridge, plus this port's contribution.

The router prompts you to add the bridge port priority. The default is 128.

```
Bridge port priority <1 - 255> (128) :
```

5 Enter the bridge port priority.

Bridge interface-specific sub-context commands
circuit (ci) (continued)

When Spanning Tree sets up designated or root ports, it uses this value to assess the importance of the port on the network, when all other factors are equal. The lower the value, the greater the port's priority.

Bridge interface-specific sub-context commands

configure (conf)

Command purpose

The `configure` command configures the Ethernet interface for bridging.

Command syntax

The syntax of the `configure` command is as follows:

```
HomeOffice: bridge eth1 configure
```

Using the command

1 To define the bridge port priority for the Ethernet interface, enter

```
bridge eth1 configure
```

The router prompts you to add the bridge port path cost. The default is 100.

```
Bridge port path cost <1 - 65535> (100) :
```

2 Enter the bridge port path cost.

Note: The value you enter is confirmed at the end of the procedure.

The router prompts you to add the bridge port priority. The default is 128.

```
Bridge port priority <1 - 255> (128) :
```

3 Enter the bridge port priority.

The bridge port priority is used by Spanning Tree to indicate to other bridges that this particular port is hierarchically inferior or superior to other ports. In this way the root port can be determined, ensuring that Ethernet is used in preference to a WAN link. This is a way of keeping network costs down.

A confirmation of the changes similar to the following appears:

```
Bridge port configuration updated :
Bridge port path cost: 300
Bridge port priority: 255
```

Bridge interface-specific sub-context commands

enabled (e)

Command purpose

The `enabled` command lets you define the bridge port state on an Ethernet interface. The bridge port state defines whether or not the bridge port can bridge.

CAUTION
Loss of connectivity
If you are administering the router remotely over a bridged interface, be careful not to disable the bridge port from which you are accessing your router. If you do, you may have to use a local administration session to restore connectivity.

Command syntax

The syntax of the `enabled` command is as follows:

```
HomeOffice: bridge eth1 enabled
```

Using the command

1 To define the bridge port state, enter

`bridge eth1 enabled`

The router prompts you to set the state. The default is enabled.

```
Bridge port state <ENABLED or DISABLED> (enabled) :
```

2 Enable the port by pressing <Enter>, or disable the port by typing `disabled`.

Bridge interface-specific sub-context commands

forward (fo)

Command purpose

The `forward` command lets you check the entries currently stored in the dynamic forwarding database for the selected interface. It does not take a parameter.

Command syntax

The syntax of the `forward` command is as follows:

```
HomeOffice: bridge <interface> forward
```

where `<interface>` is either `eth1` for the Ethernet interface or `isdn2` for the ISDN interface.

Using the command

To check the entries currently stored in the dynamic forwarding database for the Ethernet interface, enter

```
bridge eth1 forward
```

The Bridge Forwarding Table for interface `eth1` *appears. The display is similar to the following:*

```
Bridge Forwarding Table
Port : eth1                          Entries : 84
00-00-6B-80-00-72    00-00-6B-80-08-F8    00-00-6B-81-04-2C
00-00-6B-81-04-4E    00-00-6B-81-09-18    00-00-6B-81-09-5E
00-00-6B-81-10-EE    00-00-6B-81-21-06    00-00-6B-81-24-26
00-00-6B-81-2C-7C    00-00-6B-81-2C-96    00-00-6B-81-2C-A2
08-00-39-00-44-FC    08-00-39-00-46-1C    08-00-39-00-5A-D4
08-00-39-00-5A-D6    08-00-39-00-5F-46    08-00-39-00-5F-48
08-00-39-00-70-01    08-00-39-00-70-03    08-00-39-00-70-04
08-00-39-00-70-D2    08-00-39-00-7D-E6    08-00-39-00-7E-BA
08-00-39-00-80-10    08-00-39-00-86-C8    08-00-39-00-88-20
08-00-39-25-00-02    08-00-39-25-00-05    08-00-39-25-00-11
08-00-39-25-00-12    08-00-39-25-05-90    08-00-39-39-39-12
08-00-39-4A-4D-10    08-00-39-4A-4D-A0    08-00-47-00-0A-A5
-- MORE --
```

Bridge interface-specific sub-context commands

statistics (ss)

Command purpose

The `statistics` command resets or displays bridging statistics.

Command syntax

The syntax of the `statistics` command is as follows:

```
HomeOffice: bridge <interface> statistics <parameter>
```

where

- `<interface>` is either: `eth1` for the Ethernet interface or `isdn2` for the ISDN interface
- `<parameter>` is either `reset` or `frame`

Using the command

Displaying bridging statistics

To display bridging statistics for the Ethernet interface, enter

```
bridge eth1 statistics frame
```

In this example, the statistics for the Ethernet interface appear. The display is similar to the following:

```
Bridge Statistics: Port 1 (eth1)

  Total frames in                :      0 (  0.00%)
     Forwarded to port           :      0 (  0.00%)
     Port not forwarding         :      0 (  0.00%)
     Filtered dynamically        :      0 (  0.00%)
     Filtered statically         :      0 (  0.00%)
        Destination              :      0
        Source                   :      0
        Data                     :      0
```

Bridge interface-specific sub-context commands
statistics (ss) (continued)

```
Total frames out              :      86 (100.00%)
   Forwarded to port          :      86 (100.00%)
   Port not forwarding        :      0  (  0.00%)
   Filtered statically        :      0  (  0.00%)
      Destination             :      0
      Source                  :      0
      Data                    :      0
```

Resetting the statistics counter

To reset the statistics counter for the ISDN interface, enter

```
bridge isdn2 statistics reset
```

The statistics counter type for the ISDN interface is reset. The following confirmation appears:

```
Bridge statistics have been reset.
```

Bridge filter sub-context commands

The `bridge filter` sub-context lets you manage bridge filtering. Filtering is the process of testing whether a frame needs to be passed to another segment. A series of different filters or tests are used. If a frame does not pass through one of these filters (that is, it fails one of the tests), it is not passed on by the router.

Note: The bridge filter commands apply only to bridged traffic. They do not apply to IP or IPX traffic if these protocols are enabled for routing.

CAUTION
Loss of connectivity
Be extremely cautious when configuring filters that include your own Ethernet address: you may exclude yourself from your own network.

In the `bridge filter` sub-context, the command prompt is:

```
HomeOffice: bridge filter
```

The following commands for managing bridge filtering are described in this section:

Command	Shortcut	Description
data	da	Add, change, delete, or show data filters.
destination	de	Add, delete, or show destination filters.
enabled	e	Enable or disable the bridge static filters.
source	so	Add, delete, or show source filters.
statistics	ss	Show static filtering statistics.

To display a list of available commands, enter `help`. To exit to non-privileged level, enter `quit`.

Note: If you configure a filter with one of the `bridge filter` sub-context commands, you must enable it with the `enable` command before it can take effect.

Bridge filter sub-context commands

data (da)

Command purpose

The `data` command lets you configure or display data filters. Data filters filter packets by comparing their contents with a number of specified data sequences or ranges. These sequences or ranges can occur anywhere in the packet.

Command syntax

The syntax of the data command is as follows:

```
HomeOffice: bridge filter data <parameter>
```

The following table describes the parameters.

Parameter	Description	For instructions, see
add	Adds a data filter.	page 4-17
change	Changes the characteristics of a data filter.	page 4-23
delete	Deletes a data filter.	page 4-24
mode	Defines the ways in which filtering operates on the specified port.	page 4-25
show	Displays all data filters and their state.	page 4-26

Using the command

Adding a data filter

1 To add a data filter, enter

```
bridge filter data add
```

The router prompts you to enter a filter name.

```
Data filter name <up to 15 characters> :
```

Bridge filter sub-context commands
data (da) (continued)

2 Enter the name of the new data filter.

The router prompts you to set the state of the filter. The default is `enabled`*.*

```
State <DISABLED or ENABLED> (enabled) :
```

3 Enter `enabled` if you want the filter to be used immediately.

If you enable the filter and the data mode parameter is set to `specific`*, the router prompts you to discard or forward packets. The default is* `discard`*.*

If you enter `disabled`, the filter will exist but will not be used until you enable it.

The router prompts as follows:

```
Number of sequences to test <1 - 4> (1):
```

4 Enter the number of sequences to test.

```
Action <DISCARD or FORWARD> (discard) :
```

5 Choose `discard` or `forward`.

This action applies to packets on a per-filter basis. It is linked to the `Filtering criteria` prompt described below. For example, if you choose `discard` at this prompt, and the result of sequence-checking corresponds to the filtering criteria that you choose, the packet is automatically discarded.

The following prompt appears only if you choose `discard`*:*

```
Discard on receive ports <comma separated port list
up to 23 characters, ALL or NONE>

Current : (all)
New     :
```

In Specific mode (see the description of data mode in “Defining a data filter’s mode” on page 4-25), you can use data filtering to filter or forward packets as they enter or leave a port.

Bridge filter sub-context commands
data (da) (continued)

6 If you want filtering to be used as packets enter a port, type the port numbers you require. If you do not want to use filtering at this point, type none.

The following prompt appears:

```
Discard on transmit ports <comma separated port
list up to 23 characters, ALL or NONE>

Current : (all)
New     :
```

7 If you want filtering to be used as packets leave a port, type the port numbers you require. If you do not want to use filtering at this point, type none.

The following prompt appears:

```
Selection criteria <ALLMATCH, ANYDIFFERENT or
ANYMATCH> (allmatch) :
```

8 Choose the filter criteria.

The filtering criteria determines whether or not the packet is forwarded. The three options refer to the number of sequences you have tested.

Selection criteria	Description
ALLMATCH	This means a packet is forwarded or discarded (depending on the action you selected) if it meets all the filter criteria you define in the filters below.
ANYDIFFERENT	This means a packet is forwarded or discarded if it is different from any of the filter criteria you define in the filters below.
ANYMATCH	This means a packet is forwarded or discarded if it matches any of the filter criteria you define in the filters below.

The following prompt appears:

```
Number of sequences to test <1-4> (1) :
Sequence 1:
Sequence type <MATCH or RANGE> (match) :
```

Bridge filter sub-context commands
data (da) (continued)

9 Type the sequences you want to test.

Sequences are strings of hexadecimal numbers. The contents of packets are compared with these strings, and the packets are then rejected or accepted according to whether they meet the selection criteria defined.

10 Specify the type of sequences you want to test.

Use one of the following prompts:

Sequence type	Description
`MATCH`	A match sequence contains a fixed string of hexadecimal numbers. This must be repeated at the appropriate location within a packet for the packet to be accepted.
`RANGE`	A range sequence contains a hex number range. A packet must contain a number within this range, at the appropriate location, for the packet to be accepted.

If you enter `RANGE` instead of `MATCH` at this prompt, some of the subsequent prompts are different. Since this option can differ for each sequence, you can mix `range` and `match` sequence types in one filter.

These prompts are described in the following table:

Sequence type	Prompts displayed
`match` or `range`	`Sequence offset <0-1510 octets> (0) : 10` This prompt is the same for `match` and `range` sequence types. The sequence offset defines the distance from the beginning of the packet, in octets, where the comparison starts. For example, if you enter `10`, the router checks if the sequence is present, starting at the tenth octet of each packet.

—continued—

Bridge filter sub-context commands
data (da) (continued)

Sequence type	Prompts displayed

`match`	`Sequence length <1-6 octets> (4) :`
	Define the appropriate sequence length. The sequence length is measured from the offset. The longer the sequence length, the stricter the filter. For example, if you enter 2, this means that the first two octets after the offset (inclusive) are used for comparison with the mask. You can have a sequence length of up to six octets.
	`Sequence mask <8 hex digits> : 11001100`
	Enter the sequence mask in hexadecimal. This string is ANDed to the octets you have chosen to compare in the packet. The result of this action is compared to the sequence match (see next prompt). If there are any differences, the packet will not match and will be filtered (discarded).
	`Sequence match <8 hex digits> : 08000000`
	Enter the sequence match in hexadecimal. This corresponds to the type field for protocols. For example, if you want to forward only IP packets, set the forwarding mode to `ONLY`, and the match to `0800` (IP's type field). Refer to RFC 1661 for type field values of other protocols. The sequence match is compared with the sequence mask above.

—continued—	

Bridge filter sub-context commands
data (da) (continued)

Sequence type	Prompts displayed

range	`Sequence length <1, 2 or 4 octets> (4) :`
	Define the appropriate sequence length (maximum value, 4 octets). The sequence length is measured from the offset. For example, if you enter `1`, this means that the octet at the offset is used for comparison with the mask. You can have a sequence length of up to six octets.
	`Sequence lower bound <0-4294967295> : 0`
	Define the start of the sequence number range. The sequence lower and upper bounds mark the range of octets within which the router looks for the packet data. These values are inclusive.
	`Sequence upper bound <0-4294967295> : 213434677`
	Define the end of the sequence number range.

—end—	

When you have added a `MATCH` data filter, it appears as follows:

```
Data filter added:
  Name : systest1         State : enabled
  Sequence 1 : match
    Offset :   0 octets Mask : 11772299
    Size :   4 octets Match : 11332266
```

Bridge filter sub-context commands
data (da) (continued)

When you have added a RANGE data filter, it appears as follows:

```
Data filter added:
  Name        : systest2      State : enabled         d
  Sequence 1  : range
    Offset    :   2 octets     Lower bound : 0
   Size     :   4 octets    Upper bound : 213434677
```

Changing the characteristics of a data filter

1 To change the characteristics of a data filter, enter

```
bridge filter data change
```

The following prompt appears:

```
Data filter name <up to 15 characters or *> :
systest1
```

2 Enter the name of the data filter whose characteristics you want to change.

The following prompt appears:

```
Data filter name <up to 15 characters> (systest1) :
```

3 Change the name of the data filter, if required.

The following prompts are the same as for `data add` if you selected SPECIFIC mode. Refer to that description to see what values you can change.

```
State <DISABLED or ENABLED> (disabled) :
Action <DISCARD or FORWARD> (discard) :
Discard on receive ports <comma separated port list
up to 23 characters, ALL or NONE>
  Current : (all)
  New     :
Discard on transmit ports <comma separated port
list up to 23 characters, ALL or NONE>
  Current : (all)
  New     :
Selection criteria <ALLMATCH, ANYDIFFERENT or
ANYMATCH> (allmatch) :
Number of sequences to test <1-4> (1) :
```

```
Sequence 1:
  Sequence type <MATCH or RANGE> (match) :
  Sequence offset <0-1510 octets> (0) :
  Sequence length <1-6 octets> (4) :
  Sequence mask  <8 hex digits> (12345678) :
  Sequence match <8 hex digits> (23456789) :
```

The new data filter details appear.

Deleting a data filter

1 To delete a data filter, enter

```
bridge filter data delete
```

The following prompt appears:

```
Data filter name <up to 15 characters or *> :
systest2
```

2 Enter the name of the data filter you want to delete, or ***** to list all data filters, for selection.

When you press <Enter>, the filter appears.

```
  Name       : systest2     State      : disabled

 Sequence 1  : range
   Offset    :   2 octets      Lower bound : 0
   Size     :   4 octets     Upper bound : 213434677

Delete data filter <YES or NO> : yes
```

3 Enter `yes` to confirm the deletion.

The following appears:

```
Data filter deleted.
```

Bridge filter sub-context commands
data (da) (continued)

Defining a data filter's mode

1 To define the ways in which filtering operates on this port, enter

```
bridge filter data mode.
```

2 Respond to the following prompt.

```
Port filtering <GENERAL or SPECIFIC> (specific):
general
```

If you select `GENERAL`, there are two further prompts. You are not prompted for `DISCARD` or `FILTER` in each specific filter.

Port filter type	Description
`GENERAL`	The same filtering is used on all entries in the table.
`SPECIFIC`	Different filters are used for different ports. This is useful for preventing specific types of packets from going through specific ports.

The following prompt appears:

```
Forwarding mode <ONLY or EXCEPT> (except) : only
```

3 Select the forwarding mode you require.

Packets are forwarded as follows:

Forward mode	Description
`ONLY`	Only packets with the specified address are to be forwarded.
`EXCEPT`	All packets except those to specified addresses are to be forwarded.

The following prompt appears only if you selected general in step 2:

```
Ports <comma separated port list up to 23
characters, ALL or NONE>
  Current : (none)
  New     :  all
```

Bridge filter sub-context commands
data (da) (continued)

4 Define the ports on which this filter operates.

When you have changed the forwarding mode for this filter, you see

```
Forwarding mode updated:
Port filtering : GENERAL  - all filters apply to the
                            filtering ports.
Forwarding mode: ONLY     - only packets specified
by
                            these filters are being
                            forwarded.
  Filtering ports: all
```

If you selected other options in the previous prompts, the display may differ. For example:

```
Port filtering <GENERAL or
SPECIFIC>(general):specific
Forwarding mode updated:
  Port filtering : SPECIFIC - packets are being
  filtered only on the bridge ports specified in
  each filter.
```

Displaying data filters and their states

The following command

```
bridge filter data show
```

displays all data filters and their state as follows.

```
Name    State      Action    Sequences   Filter Hits

systest 1  enabled       -           1            0

Port filtering : GENERAL  - all filters apply to the
filtering ports.

Forwarding mode: EXCEPT   - all packets being
forwarded except those specified by these filters.
```

Bridge filter sub-context commands

destination (de)

Command purpose

The `bridge filter destination` command lets you configure or show destination filters. A destination filter selects packets, using their destination Ethernet address as a sorting criterion.

Command syntax

The syntax of the `destination` command is as follows:

```
HomeOffice: bridge filter destination <parameter>
```

The following table describes the parameters.

Parameter	Description	For instructions, see
add	Adds a destination filter.	page 4-27
delete	Deletes a destination filter.	page 4-28
mode	Defines how destination filtering operates.	page 4-28
show	Displays all destination filters and their setup.	page 4-29

Using the command

Adding a destination filter

1 To add a destination filter, enter

```
bridge filter destination add
```

The router prompts you to enter the Ethernet address of the destination device that is used as the sorting criterion:

```
Ethernet address <12 hex characters> :
```

Bridge filter sub-context commands
destination (de) (continued)

2 Enter the Ethernet address (12 hex characters) of the destination device. For example:

```
0000c0c6ff61
```

A message similar to the following appears:

```
Destination filter added:
Ethernet address : 0000c0c6ff61
```

Deleting a destination filter

1 To delete a destination filter, enter

```
bridge filter destination delete
```

The router prompts you to enter the Ethernet address of the destination filter that you want to delete:

```
Ethernet address <12 hex characters, or *> :
```

2 Enter the Ethernet address of the destination filter that you want to delete.

Note: Enter * to display a list of filters.

A list similar to the following appears:

```
Destination filters: 00006B800072  00006B8008F8
00006B81042C
```

After selecting a filter for deletion (for example, 00006B81042C), a message similar to the following appears:

```
Destination filter deleted:
Ethernet address : 00006B81042C
```

Defining how a destination filter operates

1 To define how a filter operates, enter

```
bridge filter destination mode
```

The router prompts you to select port filtering. The default is general.

```
Port filtering <GENERAL> (general) :
```

Bridge filter sub-context commands
destination (de) (continued)

2 Press <Enter>.

The router prompts you to select the forwarding mode. The default is `except`.

```
Forwarding mode <ONLY or EXCEPT> (except) :
```

3 Select the forwarding mode by entering `only` or `except`.

Forward mode type	Description
`only`	This means only packets with the specified address are to be forwarded.
`except`	This means all packets except those to specified addresses are to be forwarded.

If you update the filter mode, the new setup similar to the following appears:

```
Forwarding mode updated:
Port filtering :GENERAL - packets are being filtered
on all bridge ports.
Forwarding mode: ONLY   - only packets with the
specified addresses are being forwarded.
```

Displaying all destination filters

To display destination filters, enter

```
bridge filter destination show
```

Destination filters and their setup similar to the following appear:

```
Destination filters 111111111111
Port filtering : GENERAL - packets are being filtered
on all bridge ports.
Forwarding mode: EXCEPT  - all packets being forwarded
except those to the specified addresses.
```

Bridge filter sub-context commands

enabled (e)

Command purpose

The `bridge filter enabled` command lets you enable or disable all bridge static filters according to their type.

Command syntax

The syntax of the `enabled` command is as follows:

```
HomeOffice: bridge filter enabled
```

Using the command

1 To enable or disable bridge static filters, enter

```
bridge filter enabled
```

The router prompts you to select the state of destination filtering. The default is `disabled`.

```
Destination filtering <ENABLED or DISABLED>
(disabled):
```

2 To activate destination filtering, enter

```
enabled
```

The router prompts you to select the state of source filtering. The default is `disabled`.

```
Source filtering <ENABLED or DISABLED> (disabled) :
```

3 To activate source filtering, enter

```
enabled
```

The router prompts you to select the state of data filtering. The default is `disabled`.

```
Data filtering <ENABLED or DISABLED> (disabled) :
```

4 To activate data filtering, enter

```
enabled
```

If you change the filtering setup, the new setup similar to the following appears:

```
Filtering updated:
Destination filtering     : enabled
Source filtering          : enabled
Data filtering             : enabled
```

Bridge filter sub-context commands

source (so)

Command purpose

The `bridge filter source` command lets you configure or show source filters. A source filter selects packets, using their source Ethernet address as a sorting criterion.

Command syntax

The syntax of the `source` command is as follows:

```
HomeOffice: bridge filter source <action>
```

where `<action>` is either `add`, `delete`, `mode`, or `show`.

Using the command

Adding a source filter

1 To add a source filter, enter

```
bridge filter source add
```

The router prompts you to enter an Ethernet address of the source device used as the sorting criterion.

```
Ethernet address <12 hex characters> :
```

2 Enter the Ethernet address (12 hex characters) of the source device used as the sorting criterion.

A confirmation message similar to the following appears:

```
Source filter added:
Ethernet address : 00006B81042C
```

Deleting a source filter

1 To delete a source filter, enter

```
bridge filter source delete
```

The router prompts you to enter an Ethernet address of the source device you want to delete.

```
Ethernet address <12 hex characters, or *> :
```

Bridge filter sub-context commands
source (so) (continued)

2 Enter the Ethernet address (12 hex characters) of the source device you want to delete.

A confirmation message similar to the following appears:

```
Source filter deleted:
Ethernet address : 00006B81042C
```

Defining the packets to be forwarded

1 To define the packets to be forwarded, enter

```
bridge filter source mode
```

The router prompts you to specify the type of filtering (the default is `general`):

```
Port filtering <GENERAL or SPECIFIC> (general) :
```

2 Specify the type of filtering by entering `general` or `specific`.

Filter type	Description
`general`	This means the same filtering is used on all entries in the tables.
`specific`	This means different filters are used for different ports. This is useful for sending specific types of packets to specific ports.

If you specified `general`, the router prompts you to specify the forwarding mode. The default is `except`.

```
Forwarding mode <ONLY or EXCEPT> (except) :
```

3 Specify the type of filtering by entering `only` or `except`.

Filter type	Description
`only`	This means only packets with a specified address are forwarded.
`except`	This means all packets are forwarded except those to specified addresses.

Bridge filter sub-context commands
source (so) (continued)

If you change the mode setup, information similar to the following appears:

```
Port filtering : GENERAL - packets are being
filtered on all bridge ports.

Forwarding mode: ONLY   -  only packets with the
specified addresses are being forwarded.
```

Displaying source filters and their setup

To display all source filters with their setup, enter

```
bridge filter source show
```

All source filters and their setup similar to the following appear:

```
Source filters
115522884499
Port filtering : GENERAL - packets are being
filtered on all bridge ports.

Forwarding mode: ONLY    - only packets with the
specified addresses are being forwarded.

-- MORE --
```

Bridge filter sub-context commands

statistics (ss)

Command purpose

The `bridge filter statistics` command lets you display static filtering statistics for bridging.

Command syntax

The syntax of the `statistics` command is as follows:

```
HomeOffice: bridge filter statistics
```

Using the command

To display static filtering statistics for bridging, enter

```
bridge filter statistics
```

Information similar to the following appears:

```
Filter name                  Discarded       Filter
                             Packets           Hits

   Source                           5          129
   Destination                   2787         2787
   Data                             0            0
   Total                            0            0
```

Note 1: If the number of discarded packets differs from the number of filter hits, this indicates that the `ONLY` option is active for filtering.

Note 2: If the number of discarded packets equals the number of filter hits, this indicates that the `EXCEPT` option is active for filtering.

Bridge span sub-context commands

The `bridge span` sub-context lets you manage the Spanning Tree Algorithm. This algorithm blocks some bridge ports so that there is only one path between any two devices on the network. This prevents loops and adds resilience, as some links become standby links. However, using the Spanning Tree Algorithm may increase traffic across links, and it also lengthens paths between devices. As a result, traffic may be delayed.

In the `bridge span` sub-context, the command prompt is:

```
HomeOffice: bridge span
```

The following commands are described in this section:

Command	Shortcut	Description
configure	conf	Configure Spanning Tree priorities.
enabled	e	Enable or disable the Spanning Tree Algorithm.
port	po	Show the Spanning Tree port status.
reset	rst	Reset the Spanning Tree and Path Optimization algorithms.
status	st	Display Spanning Tree status.

To display a list of available commands, enter `help`. To return to non-privileged mode, enter `quit`.

Bridge span sub-context commands

configure (conf)

Command purpose

The `bridge span configure` command lets you configure the priority of your router. The bridge priority is used by Spanning Tree to indicate to other bridges that this particular bridge is hierarchically inferior or superior to other bridges. In this way the root bridge can be determined, ensuring that Ethernet is used in preference to a WAN link. This is a way of keeping network costs down.

Command syntax

The syntax of the `configure` command is as follows:

```
HomeOffice: bridge span configure
```

Using the command

Configuring bridge priority

Note: In this procedure, the range of values shown in parentheses varies depending on the values defined in the root bridge.

1 To configure bridge priority, enter

```
bridge span configure
```

The router prompts you to specify a bridge priority value.

```
Bridge priority <0-65535> (32767) :
```

2 Specify the bridge priority by entering a number in the indicated range.

The bridge priority shows the importance of the router on the network. The bridge priority generally determines which bridge/router or bridge is the root or designated bridge, although path cost and port priority (not affected by this command) are also taken into account.

The current default value is shown in parentheses. The lower the value, the greater the router's priority.

The router prompts you to specify a bridge forward delay value.

```
Bridge forward delay <4-30> (15) :
```

Bridge span sub-context commands
configure (conf) (continued)

3 Specify the bridge forward delay by entering a number in the indicated range.

The bridge forward delay value is the time in seconds that a router spends listening and then learning before it starts forwarding. If this value is set to five seconds, for example, the router listens for five seconds, then learns for a further five seconds before starting to forward packets.
A long delay gives the router more time to learn addresses so that when the device begins forwarding, fewer irrelevant frames are included. It also increases the possibility that network topology will be stable when it starts forwarding.

The current default value is shown in parentheses.

The router prompts you to specify the bridge maximum age value.

```
Bridge max age <6-28> (20) :
```

4 Specify the bridge maximum age by entering a number in the indicated range.

The bridge maximum age is the time, in seconds, that a router holds information it receives from other devices. If a hello message is not received from a device within this time, the device is assumed to be no longer present. This leads to network reconfiguration. The maximum age must be long enough to let hello messages through. On a busy network, you may need a higher value.

The current default value is shown in parentheses.

The router prompts you to specify the bridge hello time value.

```
Bridge hello time <1-9> (2) :
```

5 Specify the bridge hello time by entering a number in the indicated range.

The bridge hello time is the interval in seconds between hello messages. These are sent out regularly by the Root Bridge.

The current default value is shown in parentheses.

The router prompts you to specify the multicast (group) address.

```
Group address <12 hex characters or DEFAULT>  :
```

Bridge span sub-context commands
configure (conf) (continued)

6 If you want to set up a domain, enter its multicast address by entering either 12 hex characters or `default` to accept the default address.

The multicast address is used by Spanning Tree. The default address is `0180C2000000`.

When you have set values for all the parameters, the updated configuration appears.

```
Spanning tree configuration updated:

Bridge priority      : 32767
  Bridge forward delay : 20
  Bridge max age       : 25
  Bridge hello time    : 1
  Group address        : 0180C2000000  (default)
```

Displaying the current Spanning Tree configuration

To display the current Spanning Tree configuration, enter

```
bridge span configure show
```

The current Spanning Tree configuration similar to the following appears:

```
bridge span configure show

Bridge priority      : 32767
  Bridge forward delay : 16
  Bridge max age       : 21
  Bridge hello time    : 1
  Group address        : 0180C2000000  (default)
```

Bridge span sub-context commands

enabled (e)

Command purpose

The `bridge span enabled` command lets you enable or disable the Spanning Tree Algorithm.

Command syntax

The syntax of the `enabled` command is as follows:

```
HomeOffice: bridge span enabled
```

Using the command

1 To enable or disable the Spanning Tree Algorithm, enter

```
bridge span enabled
```

The router prompts you to specify the state.

```
Spanning tree <ENABLED or DISABLED> (enabled):
```

2 Specify the state by entering `enabled` or `disabled`.

When you enable or disable Spanning Tree, there is a short delay before you can continue using your router; this is because the router is reconfiguring itself.

When you change the Spanning Tree configuration, information similar to the following appears:

```
Spanning tree updated:
       Spanning tree : enabled
```

Bridge span sub-context commands

port (po)

Command purpose

The `bridge span port` command displays Spanning Tree port status information.

Command syntax

The syntax of the `port` command is as follows:

```
HomeOffice: bridge span port
```

Using the command

To display Spanning Tree port status information, enter

```
bridge span port
```

Information similar to the following appears:

```
Port 1 : eth1
   State                                  : forwarding
   Cost                                   : 100
   Designated bridge - priority, address  : 32767,050800390070D2
   Designated port - priority, ID         : 0, 2
   Designated port cost                   : 0

 Port 2 : isdn2
   State                                  : forwarding
   Cost                                   : 15625
   Designated bridge - priority, address  : 32767,0800390087D4
   Designated port - priority, ID         : 233, 2
   Designated port cost                    : 100
```

Bridge span sub-context commands
port (po) (continued)

The following table describes the states that can be shown after the port name.

State	Description
Forwarding	Normal state; the port is forwarding packets.
Listening	When the router is first switched on, it listens for Spanning Tree packets and learns the network topology.
Learning	The router adds entries to the Forwarding table.
Blocking	The port is blocked by Spanning Tree.
Disabled	The port is disabled by the user.

Bridge span sub-context commands

reset (rst)

Command purpose

The `bridge span reset` command is used to reset the Spanning Tree.

Command syntax

The syntax of the `reset` command is as follows:

```
HomeOffice: bridge span reset
```

Using the command

1 To reset the Spanning Tree, enter

```
bridge span reset
```

The router prompts you to select an interface to reset.

```
Interface to reset  <eth1 or isdn2> (all) :
```

2 Select an interface to reset by entering `eth1` or `isdn2` or `all`.

When you have reset the required interface(s), a message similar to the following appears:

```
Spanning tree reset on eth1 interface.
```

When you reset Spanning Tree, there is a short delay before you can continue using your router; this is because the router has to reconfigure itself.

Bridge span sub-context commands

status (st)

Command purpose

The `bridge span status` command allows you to display the status of Spanning Tree on your router.

Command syntax

The syntax of the `status` command is as follows:

```
HomeOffice: bridge span status
```

Using the command

To display the status of Spanning Tree on your router, enter

```
bridge span status
```

Information similar to the following appears:

```
                Spanning Tree Status

Local unit:
    Address           : 0800390087D4
    Priority          : 32767
    Forward delay     : 15
    Max age           : 20
    Hello time        : 2
    Root port         : 1 (eth1)
    Root path cost    : 100
    Group address     : 0180C2000000 (default)

  Root unit:
    Address           : 0800390070D2
    Priority          : 95
    Forward delay     : 4
    Max age           : 21
    Hello time        : 4

  Topology stable for :  3h 50m 26s
```

IP context shell commands

The `ip` context lets you manage IP routing. Commands are grouped into sub-contexts. The following sub-contexts are described in this section:

IP context	Description
general	Configure IP parameters that apply, regardless of interface.
eth1	Configure IP parameters specific to an Ethernet interface.
isdn2	Configure IP parameters specific to an ISDN interface.
filter	Configure IP filtering. (These commands are grouped in `ip filter` sub-context for ease of location.)

IP general sub-context commands

The `IP general` sub-context lets you manage those aspects of IP routing that are not interface-dependent.

In the `IP general` sub-context, the command prompt is:

```
HomeOffice: ip general
```

The following commands are described in this section:

Command	Shortcut	Description
address	ad	Set up Internet addressing information for bridging interfaces.
arp	ar	Display the Address Resolution Protocol table for all bridged interfaces.
dhcp	d	Configures the Dynamic Host Configuration Protocol (DHCP) settings for the router's built-in DHCP server.
enabled	e	Enable or disable IP on bridged interfaces.
forward	fo	Display the Routing table.
icmp	i	Enable or disable Internet Control Message Protocol (ICMP) for bridging interfaces.
relay	re	Create a table of destinations for packets that will be routed off bridge-only interfaces.
rip	ri	Set up the Routing Information Protocol (RIP) for bridging interfaces.
route	ro	Modify the static Routing Table.
statistics	ss	Display IP routing statistics.

To display a list of available commands, enter `help`. To return to non-privileged level, enter `quit`.

IP general sub-context commands

address (ad)

Command purpose

The `IP general address` command sets up an IP address of your router for interfaces that are used only for bridging.

Command syntax

The syntax of the `address` command is as follows:

```
HomeOffice: ip general address <parameter>
```

where `<parameter>` is either blank (to set up an address) or `show` (to display the current address).

Using the command

Specifying an IP address for bridging

1 To specify an IP address for bridging-only interfaces, enter

```
ip general address
```

The router prompts you to specify the IP address.

```
Modifying the IP address for bridged interfaces
New IP address <4 bytes b1.b2.b3.b4 or
NONE> (<not assigned>) :
```

2 Enter the IP address.

Note: The IP address you enter must be unique and should conform to the addressing scheme used on your own network.

The router prompts you to specify the subnet mask.

```
Subnet mask <No of contiguous bits (8-32),
b1.b2.b3.b4 or NONE> (none) :
```

3 Enter the subnet mask address.

Unless you are dealing with a complicated network, enter `none` for the subnet mask. Otherwise, consult the administrator for the appropriate network to find out how it is subnetted.

The router prompts you to specify the broadcast style.

```
Broadcast style for host part
(ONES or ZEROS) (ones):
```

IP general sub-context commands
address (ad) (continued)

4 Specify the style of broadcasts that your host supports.

Broadcasts can be made as all ones or all zeros.

The router prompts you to specify whether you want broadcasts forwarded onto the LAN.

```
Forward broadcasts <ON or OFF> (off) :
```

5 Specify whether you want broadcasts forwarded onto the LAN.

When you have finished, the IP address information similar to the following appears.:

```
IP Bridge address updated:

IP address                 : 43.000.029.187
   Subnet mask             : 255.000.000.000
   IP                      : enabled
   Broadcast style         : ones
   Forward broadcasts      : on      (current = off)
```

Note: If you make changes to the Internet address(es), these take effect only after you restart the router.

6 To restart the router, enter

```
quit
```

When you are asked if you want to restart the router, enter `yes`.

Displaying IP addresses on interfaces

To display the IP addresses for each of the router's interfaces, enter

```
ip general address show
```

IP general sub-context commands

arp (ar)

Command purpose

The router uses the Address Resolution Protocol (ARP) to translate Internet addresses into Ethernet addresses. The `IP general arp` command displays the physical interface and all logical addresses on it.

Command syntax

The syntax of the `arp` command is as follows:

```
HomeOffice: ip general arp
```

Using the command

To display the address conversion table for logical interface addresses, enter

```
ip general arp
```

If you have not set an IP address on the Ethernet interface(s), the following message appears:

```
An IP address has not been assigned to this interface
yet.
```

If you have set an IP address on the Ethernet interface(s), the following information appears:

```
ARP table for logical interface address 2.002.002.002

ARP Table
Internet Address     Ethernet Address       Life
   2.002.002.147          080020101E11       10 mins
```

IP general sub-context commands

dhcp (d)

Command purpose

The `ip general dhcp` command configures the Dynamic Host Configuration Protocol (DHCP) settings for the HomeOffice Router's built-in DHCP server. In most cases, your network administrator can provide you with the parameters for the `dhcp` command.

The DHCP server acts with both Multi-User and Single-User DIAT. It allows you to configure your PC to view and access other hosts on the network, and supports the following types of servers:

- Domain Name Servers (DNS)
- Windows Internet Naming Service (WINS)

Note: DHCP works in conjunction with DIAT. Therefore, a DIAT circuit must be activated for DHCP to operate. However, if you wish to enable DHCP when your HomeOffice Router has no circuits configured with DIAT, you can still do so. To do this, enable DIAT on a circuit you are not using, for example, the admin circuit.

Command syntax

The syntax of the `dhcp` command is as follows:

```
HomeOffice : ip general dhcp
```

Using the command

1 To configure DHCP on the router, enter `ip general dhcp`.

The router prompts as follows:

```
DHCP <ENABLED or DISABLED> (enabled) :
```

2 Select `enabled` or `disabled`.

DHCP is enabled by default. It is only effective if the router has at least one circuit configured with DIAT.

The router prompts as follows:

```
Domain Name <up to 43 characters or NONE> (NONE) :
```

IP general sub-context commands
dhcp (d) (continued)

3 Enter the name of the domain of which you want your host to be part.

For example, if your network is part of the domain called yourcompany.com, you would enter that value here.

The router prompts as follows:

```
Primary DNS Address <b1.b2.b3.b4, or NONE>
(NONE) : 89.0.12.13
```

4 Enter the IP address on the remote network of the primary domain name server you want to use.

The router prompts as follows:

```
Secondary DNS Address <b1.b2.b3.b4, or NONE>
(NONE) : 89.0.12.15
```

5 Enter the IP address on the remote network of the secondary domain name server you want to use.

The router prompts as follows:

```
Primary WINS Address <b1.b2.b3.b4, or NONE>
(NONE) : 89.0.15.11
```

6 Enter the IP address on the remote network of the primary Windows Internet Naming Service server you want to access.

The router prompts as follows:

```
Secondary WINS Address <b1.b2.b3.b4, or NONE>
(NONE) : 89.0.15.12
```

7 Enter the IP address on the remote network of the secondary Windows Internet Naming Service server you want to access.

When you have entered all the parameters, you see the following:

```
DHCP Parameters updated:

DHCP Network Parameters

DNS Address Primary : 89.0.12.13

DNS Address Secondary : 89.0.12.15

WINS Address Primary : 89.0.15.11

WINS Address Secondary : 89.0.15.12
```

IP general sub-context commands

enabled (e)

Command purpose

The `ip general enabled` command applies to bridging interfaces, and activates or deactivates IP.

Command syntax

The syntax of the `enabled` command is as follows:

```
HomeOffice: ip general enabled [show]
```

Using the command

Enabling IP

1 To enable IP, enter

```
ip general enabled
```

The router prompts you to choose the status.

```
Enable IP on bridged interfaces <YES or NO> (yes) :
```

2 Enter `yes` if you want IP to be enabled for bridging interfaces, or no if you want it to be disabled.

Note: The change does not take effect until you restart the router.

Displaying IP status

To show the current IP status, enter

```
ip general enabled show
```

The routing interfaces on which IP is enabled, as well as the current bridge IP state appear. The arrow shows you the current interface.

```
                IP Protocol Table
   Interface        Enabled       Current

   134.196.6.4      no             disabled
=> 191.193.77.8     yes            enabled
   200.200.7.1      yes            enabled
    127.0.0.1           no                disabled
```

IP general sub-context commands

forward (fo)

Command purpose

The `IP general forward` command lets you check the information currently stored in the IP forwarding table.

Command syntax

The syntax of the `forward` command is as follows:

```
HomeOffice: ip general forward
```

Using the command

To check the information currently stored in the IP forwarding table, enter

```
ip general forward
```

Information similar to the following appears.:

```
IP Routing Table

Host or Network  Route Mask      Next Hop Router  Metric Source
4.000.000.000    255.000.000.000         -         1     direct
40.000.000.000   255.000.000.000         -         1     direct
41.000.000.000   255.000.000.000         -         1     direct
42.000.000.000   255.000.000.000         -         1     direct
192.168.169.000  255.255.255.000         -         1     direct
```

In addition to entries entered statically using `route add`*, the IP routing table contains information provided by RIP and ICMP. Metric is the RIP metric (hop count).*

The Route Mask column shows any subnet masks that have been set up. If you have not set up any subnet masks, this column has an `n/a` *entry.*

The Source column also shows any directly connected networks as `direct`.

IP general sub-context commands

icmp (i)

Command purpose

The `IP general icmp` command lets you define what the router does with Internet Control Message Protocol (ICMP) redirect messages on this interface. ICMP provides information about why IP packets fail to get to their destinations. In the `IP general` context, the `icmp` command applies only to interfaces used for bridging, where it changes the current values.

Command syntax

The syntax of the `icmp` command is as follows:

```
HomeOffice: ip general icmp [show]
```

Using the command

Managing ICMP on interfaces used for bridging

1 To manage ICMP on interfaces used for bridging, enter

```
ip general icmp
```

The router prompts you to specify if ICMP redirects should be transmitted on bridged interfaces.

```
Transmit ICMP redirects on bridged
interfaces <ON or OFF> (on):
```

2 If you want to stop the router from sending ICMP redirects on a WAN interface to save bandwidth, enter `off`.

Note: This should not be necessary on a LAN interface.

Otherwise enter `on`.

The router prompts you to specify if ICMP redirects on bridged interfaces are monitored.

```
Listen for ICMP redirects on bridged
interfaces <ON or OFF> (off):
```

To listen for ICMP redirects means the router monitors incoming ICMP redirects and uses information provided by ICMP to update its Routing table.

IP general sub-context commands
icmp (i) (continued)

3 Specify whether ICMP redirects on bridged interfaces are monitored by entering on or `off`.

If you select `off`, the router ignores incoming ICMP redirects and does not use information provided by ICMP to update its Routing table.

Note: If you are running RIP (see the `rip` command), the router automatically ignores ICMP redirects.

If you change the ICMP parameters, information similar to the following appears:

```
ICMP redirects not updated:
  Interface               : bridge
  Transmit ICMP redirects  : on
  Listen ICMP redirects     : off
```

Displaying current ICMP redirects

To display current ICMP redirects, enter

```
ip general icmp show
```

Information similar to the following appears:

```
ICMP Redirects
    Interface          Transmit          Listen
   192.168.169.168        off              off
    40.000.000.001        off              off
    41.000.000.001        off              off
    42.000.000.001        off              off
=>    4.005.008.009           on                 off
```

IP general sub-context commands

relay (re)

Command purpose

The `IP general relay` command creates a table of destinations for broadcasts that are routed to remote destinations from bridge-only interfaces.

Command syntax

The syntax of the `relay` command is as follows:

```
HomeOffice: ip general relay <action>
```

where `<action>` is either `add`, `change`, `delete`, `enable`, or `show`.

Using the command

Adding destinations

1 To add a destination, enter

```
ip general relay add
```

The router prompts you to enter the IP address.

```
IP address <4 bytes b1.b2.b3.b4> :
```

2 Enter either

- the IP address of the NetBIOS or BootP server from which you want to receive broadcasts, or
- the broadcast address of the network on which the server is located

Note: You would be most likely to use the broadcast address if there are several servers on one network.

The router prompts you to specify if UDP broadcasts are to be forwarded.

```
Forward all UDP broadcasts <ON or OFF> (off) :
```

IP general sub-context commands
relay (re) (continued)

3 Do the following:

If you want to	Then
forward all types of UDP broadcasts, including NetBIOS and BootP	enter on.
forward NetBIOS or BootP packets	enter `off`.

If you enter `off`, the router prompts for the following:

```
Forward NetBIOS packets <ON or OFF> (off) :
Forward BOOTP/DHCP packets <ON or OFF> (off) :
```

4 Enable forwarding of NetBIOS or BootP packets, as required.

The details of the relay address that you added appear:

```
Relay address added:
   Address                    : 85.0.0.2
   Forward all UDP broadcasts  : off
   Forward NetBIOS packets     : on
   Forward BOOTP/DHCP packets   : off
```

Note: The maximum number of entries in the Relay Forwarding Table is 16 per interface.

Changing the details of relay addresses

1 To edit the details of an existing relay address, enter

```
ip general relay change
```

The router prompts you to specify the relay address to change.

```
Relay address <IP address or *> :
```

2 Enter the IP address to change.

The router prompts for the new IP address.

```
New IP address <4 bytes b1.b2.b3.b4> (85.0.0.2):
```

3 Enter the new IP address.

The router prompts you to specify if UDP broadcasts are to be forwarded.

```
Forward all UDP broadcasts <ON or OFF> (off) :
```

IP general sub-context commands
relay (re) (continued)

4 Do the following:

If you want to	Then
forward all types of UDP broadcasts, including NetBIOS and BootP	enter on.
forward NetBIOS or BootP packets	enter `off`.

If you enter `off`, the router prompts for the following:

```
Forward NetBIOS packets <ON or OFF> (off) :
Forward BOOTP/DHCP packets <ON or OFF> (off) :
```

5 Enable forwarding of NetBIOS or BootP packets, as required.

The details of the relay address that you added appear.

```
Relay address added:
   Address                    : 85.0.0.2
   Forward all UDP broadcasts  : off
   Forward NetBIOS packets     : on
   Forward BOOTP/DHCP packets   : off
```

Note: The maximum number of entries in the Relay Forwarding Table is 16 per interface.

Deleting relay addresses

1 To delete a relay address, enter

```
ip general relay delete
```

The router prompts you to specify the relay address to delete.

```
Relay address <IP address or *> : *
```

2 Enter the address that you want to delete.

Details of the address appear:

```
Relay address to delete:
   Address                    :   2.002.002.002
   Forward all UDP broadcasts  : off
   Forward NetBIOS packets     : off
   Forward BOOTP/DHCP packets  : off
```

3 When you are asked to confirm the deletion, enter `yes` to delete or `no` to cancel.

IP general sub-context commands
relay (re) (continued)

Enabling relay addresses

The `enable` parameter determines whether or not IP relay addresses are used. If you disable IP relay addresses, any relay addresses that you set using the add parameter are not used.

1 To enable or disable IP relay addresses, enter

```
ip general relay enable
```

The following prompt appears:

```
Use IP relay addresses <ON or OFF> (off) :
```

2 Enter `on` to enable or `off` to disable IP relay addresses.

Note: You must restart the router for this change to take effect.

Displaying relay address details

The show parameter displays details of the IP Relay Addresses to which packets are routed from bridge-only interfaces.

To display details of IP Relay Addresses, enter

```
ip general relay show
```

Information similar to the following appears:

```
                IP Relay Addresses
IP Address              Protocols
 88.000.000.001         All UDP broadcasts
 88.000.000.002          NetBIOS
```

IP general sub-context commands

rip (ri)

Command purpose

The IP general `rip` command enables and disables the Routing Information Protocol (RIP), which is the dynamic routing protocol used on TCP/IP networks. This command lets you enable and disable RIP for IP on interfaces used only for bridging.

Command syntax

The syntax of the `rip` command is as follows:

```
HomeOffice: ip general rip [show]
```

Using the command

Enabling RIP

1 To enable or disable RIP, enter

`ip general rip`

The router prompts for the following information:

```
RIP on bridged interfaces <ON or OFF> (off) :
```

2 Enter `on` to activate RIP.

The following appears:

```
Interface cost <1 -15 or INFINITY> (1) :
```

The Interface Cost 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.

3 Enter a value between `1` and `15` or `infinity`.

If	Then
an interface gives access to a particularly expensive WAN	you may want to set the parameter quite high.
you want to force traffic to use a particular route	set the value quite low.

IP general sub-context commands
rip (ri) (continued)

The following appears:

```
Triggered Retry Count <5 - 100 or INFINITY> (5) :
```

4 Define the number of times that RIP tries to connect with RIP on the destination router, if they cannot communicate (for example, due to incorrect configuration).

The following appears:

```
Triggered Retry Interval in minutes <1 - 10> (1)
```

5 Define the time interval between triggered retry attempts.

The following appears:

```
Include default routes in RIP packets <YES or NO>
(yes) :
```

6 Respond as required.

The following appears:

```
Ignore incoming RIP updates <YES or NO> (no) :
```

7 Respond as required.

The following display appears.

```
Routing Information Protocol updated:
  Interface               : bridge
  RIP                     : off
  Cost                    : 1
  Triggered Retry Count   : 5
  Triggered Retry Interval : 1
  Include default routes  : yes
  Ignore RIP Updates      : no
```

IP general sub-context commands
rip (ri) (continued)

Displaying RIP status

To display the status of RIP on all of the router's interfaces, enter `ip general rip show`.

You see:

```
Routing Information Protocol
Interface      RIP   Cost  Retry     Retry      Include       Warn
                           Count   Interval  Default Routes

168.169.168    off    1      5         1         yes           -
41.000.000.001 off    1      5         1         yes           -
42.000.000.001 off    1      5         1         yes           -
=>5.008.009    off infinity  -         -          -            -
```

Note: The arrow points to the current interface.

IP general sub-context commands

route (ro)

Command purpose

The `IP general route` command configures the static entries in the Routing table. Statically entered routing addresses are stored permanently in the router's Routing table and define the routes by which the router reaches remote networks. `Route` lets you enter this information explicitly. The Routing table also contains information provided by RIP and ICMP.

Command syntax

The syntax of the `route` command is as follows:

```
HomeOffice: ip general route <action>
```

where `<action>` is either `add`, `change`, `delete`, `learn`, or `show`.

Using the command

Adding routes

You can add up to three routes to the same destination network. You cannot start adding routes until you have assigned the necessary Internet addresses to the router.

1 To add a static route to the routing table, enter the following and press <Enter>.

```
ip general route add
```

You see:

```
Remote network or host <Internet address
or DEFAULT >:
```

2 Enter the address of the final destination network or host.

This must not be a network to which the router is directly connected. If you enter `*`, the router lists possible networks and hosts from the IP Name Table.

The router prompts you to enter the next hop router Internet address.

```
Next hop router <Internet address,
Interface name > :
```

IP general sub-context commands
route (ro) (continued)

3 Enter the address of the first router down the line towards that network.

This router must be on a network to which the router is directly connected.

The router prompts you to enter the number of hops to the destination network.

```
RIP metric <1 - 15> (2) :
```

4 Enter the metric, that is, the number of hops it takes to reach the destination network.

Packets are sent over the route with the lowest metric. 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.

Changing routes

To change a static entry in the Routing table, enter `ip general route change` followed by the Internet address of the remote network or host.

If you are not sure exactly which entries are stored in the Routing table, enter `route change *` to list the possible Internet addresses.

The prompts are the same as for `route add`. Enter a new value or press <Enter> to leave a value unchanged. If there is more than one entry for the host or network you specify, each entry appears in turn.

Deleting routes

To delete an entry in the Routing table, enter `ip general route delete` followed by the entry's Internet address.

The router displays the entry and does not delete it until you respond `yes` to the prompt.

If you are not sure exactly what is in the Routing table, enter `route delete *` to list the possible Internet addresses.

IP general sub-context commands
route (ro) (continued)

Storing dynamically entered routes as static routes

Use `ip general route learn` if you have entered routes in the Routing table manually, that is, dynamically, and want to store them for future use. The router looks for individual dynamic entries and asks you to confirm that you want them to be stored as static entries.

Displaying routes

To display static routing entries, enter `ip general route show`.

When you press <Enter>, you see:

```
IP Routing Table

Host or Network  Route Mask      Next Hop Router Metric Cost Warn
1.001.001.001    255.255.255.255 2.000.676.001    2      1    -
```

Note: The Route Mask column shows any subnet masks that have been set up. If you have not set up any subnet masks, this column has an `n/a` entry.

Alternatively, use the `forward` command to display the entire Routing table.

IP general sub-context commands

statistics (ss)

Command purpose

The `IP general statistics` command displays information on the IP routing carried out by the router. Error and dropped datagram totals should remain low. If they rise suddenly, this indicates a problem with your network.

Command syntax

The syntax of the `statistics` command is as follows:

```
HomeOffice: ip general statistics
```

Using the command

To display IP routing statistics, enter `IP general statistics`.

The display looks like this:

```
Total datagrams received :     186450
  For applications  :           90915 ( 48.76%)
  For forwarding    :           18378 (  9.85%)
  Dropped datagrams :
    Header error      :             4 (  0.00%)
    Address error     :             0 (  0.00%)
    Unknown protocol  :             0 (  0.00%)
    Other Reason      :             0 (  0.00%)

Total datagrams sent :          51021
  From applications  :           32643 ( 63.97%)
  Dropped datagrams  :
    Lack of route    :         22035 ( 43.18%)
    Other Reason     :             0 (  0.00%)

Datagrams fragmentated :            0 (  0.00%)  Fragments : 0
  Unable to fragment   :            0 (  0.00%)

Fragments received     :            0 (  0.00%)  Datagrams: 0
  Unable to re-assemble:            0 (  0.00%)
```

IP interface sub-context commands

The HomeOffice Router has a sub-context for each of its physical interfaces. The commands in these sub-contexts let you configure the specific interface to route IP.

In the `IP <interface>` sub-context, the command prompts are:

```
HomeOffice: ip eth1
```

```
HomeOffice: ip isdn2
```

for the Ethernet and ISDN interfaces respectively.

The following commands are described in this section:

Command	Shortcut	Interface	Description
address	ad	eth1 isdn2	Allocates an interface's Internet address.
arp	ar	eth1	Displays the address conversion table.
association	as	isdn2	Relates an IP address to a circuit using the circuit name.
circuit	ci	isdn2	Relates a circuit to an IP address using the circuit name.
diat	d	eth1 isdn2	Configures Dynamic IP Address Translation (DIAT) on the ISDN interface.
enabled	e	eth1 isdn2	Enables or disables IP routing on this interface.
icmp	i	eth1 isdn2	Enables or disables Internet Control Message Protocol (ICMP) on this interface.
lookup	l	isdn2	Displays the last 20 lookup failures in the Association table.

—continued—

Command	Shortcut	Interface	Description
relay	re	eth1	Creates a table of destinations for packets that will be routed off the Ethernet to remote destinations.
rip	ri	eth1 isdn2	Enables or disables Routing Information Protocol (RIP) on this interface.
spoof	sp	eth1	Enables or disables spoofing of certain data packets that are sent periodically by a LAN host to determine if other hosts are still connected.
—end—			

To display a list of available commands, enter `help`. To exit back to non-privileged level, enter `quit`.

The `arp` and `relay` commands are only available in `Ethernet` sub-contexts. The `association`, `circuit`, and `lookup` commands are available only in `ISDN` sub-contexts.

> ***Note:*** Commands relating to filtering are grouped together in the `ip filter` sub-context.

IP interface sub-context commands

address (ad)

Command purpose

The `ip <interface> address` command is available in all contexts, and sets up Internet addresses for the Ethernet or ISDN interface. You can assign more than one Internet address to each interface by using IP Multihoming. This allows the router to run more than one logical network out of the same physical network.

Command syntax

The syntax of the `address` command is as follows:

```
HomeOffice: ip <interface) address <action>
```

where `<interface>` is either `eth1` or `isdn2`, and `<action>` is either `add`, `change`, `delete`, or `show`.

Using the command

ip <interface> address

When you type `address`, the following prompt appears:

```
Interface IP Addresses <ADD, CHANGE, DELETE
or SHOW> :
```

Adding an IP address for the interface

1 To add a logical IP address, enter `add`.

The router prompts you for the new address. The IP address you enter must be unique and should conform to the addressing scheme used on your own network.

```
New IP address <4 bytes b1.b2.b3.b4 or NONE>
<not assigned>) :
```

2 Enter the address or enter `none`.

The router prompts you for the subnet mask address.

```
Subnet mask <No of contiguous bits (8-32),
b1.b2.b3.b4 or NONE> (none) :
```

IP interface sub-context commands
address (ad) (continued)

3 Unless you are dealing with a complicated network, enter `none` for the subnet mask. Otherwise, consult the Administrator for the appropriate network to find out how it is subnetted. The final three prompts only appear for the LAN interface:

```
Broadcast style for host part (ONES or
ZEROS) (ones):
```

4 Select the broadcast style supported by your hosts.

Broadcasts can be made as all ones or all zeros.

The following prompt appears:

```
Forward broadcasts <OFF or ON> (off):
```

5 Specify whether you want broadcasts forwarded onto the LAN.

When you have completed the configuration, the details of the new IP addresses appear:

```
eth1 IP address updated:

IP address        : 11.001.001.000  (current = <not assigned>)
Subnet mask       : 255.000.000.000 (current = <not assigned>)
IP                : enabled         (current = disabled)
Broadcast style   : ones
Forward broadcasts: off
This change will take effect the next time the unit is
“software started” using “top boot”.
```

Note: Any change to the Internet address(es) takes effect only after you restart the router. When you have finished setting the addresses, enter `quit`. When you are asked if you want to restart the router, type `yes`.

Deleting IP addresses

The `ip <interface> address delete` command allows you to delete a selected IP address. You are prompted to confirm or cancel the deletion.

```
Delete IP Address <YES or NO> :y
```

The deletion takes effect the next time the unit software is restarted using `top boot`.

IP interface sub-context commands
address (ad) (continued)

Displaying IP address information for the interface

The `ip <interface> address show` command displays only the IP address information for the sub-context you are currently in. For example:

```
IP Address Table
Interface   IP Address    Subnet Mask    State    Broadcast    Running
                                                    Style      Status
=> eth1       70.1.1.0      255.0.0.0    enabled   ones       active
              10.1.1.0      255.0.0.0    enabled   ones       active
              11.1.1.0      255.0.0.0    enabled   ones       active
```

The `Running Status` column shows the status of each logical interface within a physical interface. Possible entries can be:

Status	Description
active	This logical interface is currently running and active.
restart	You must restart the router before this interface becomes active. (This normally applies to a newly added address.)
deleted	You have deleted this address. However, it will continue to run until you restart the router.

Displaying all IP addresses

The `ip <interface> address show all` command displays the router's Internet addresses for all interfaces.

IP interface sub-context commands

arp (ar)

Command purpose

The router uses the Address Resolution Protocol (ARP) to translate Internet addresses into Ethernet addresses. The `ip eth1 arp` command applies to a physical interface and all logical addresses on it.

Command syntax

The syntax of the `arp` command is as follows:

```
HomeOffice: ip eth1 arp
```

Using the command

Activating ARP on the interface

If you have not set an IP address on the Ethernet interface(s), you see the following warning message when you type `arp` at the above prompt.

```
An IP address has not been assigned to this interface
yet.
```

Use the `arp` command to display the address conversion table for logical interface addresses.

The display looks similar to the following:

```
ARP table for logical interface address   2.002.002.002

ARP Table
Internet Address     Ethernet Address       Life
     2.002.002.147        080020101E11        10 mins
     2.002.002.060        08004E03505F         7 mins


ARP table for logical interface address   3.003.003.003

ARP Table
Internet Address     Ethernet Address       Life
     3.003.003.126        0000C08C3253         7 mins
     3.003.003.214        00006B812908         1 mins
     3.003.003.242        080039005B7D         3 mins
```

IP interface sub-context commands
arp (ar) (continued)

The following table describes the fields.

Field	Description
`Internet address`	This is the IP address that was assigned to the router.
`Ethernet Address`	This is the router's MAC address.
`Life`	This is the length of time in which the entry will remain in the ARP table before being removed by the HomeOffice Router. The default is ten minutes.

IP interface sub-context commands

association (as)

Command purpose

The `ip isdn2 association` command lets you relate an IP address to a circuit by using its circuit name.

Command syntax

The syntax of the `association` command is as follows:

```
HomeOffice: ip isdn2 association <action>
```

where `<action>` is either `add`, `change`, `delete`, or `show`.

Using the command

Adding an association

1 To create a new association for this interface, enter

```
ip isdn2 association add
```

The router prompts as follows:

```
Internet address <4bytes b1.b2.b3.b4 or unnumbered,
name or *>:
```

2 Enter the IP address of the destination you want to reach.

The router prompts as follows:

```
Circuit Name <Up to 15 Characters or *>:
```

3 Specify the circuit to be used.

The circuit must be accessible from this interface.

The router prompts as follows:

```
IP <ENABLED or DISABLED> (enabled) :
```

4 Enable the interface.

Note: You can also use the `association` command to disable IP routing on this circuit.

The router prompts as follows:

```
RIP Mode <STANDARD, TRIGGERED, DELTA,
or OFF> (off) :
```

IP interface sub-context commands
association (as) (continued)

5 Select the RIP mode you require for this association.

The router prompts as follows:

```
RIP Version <1, 2 or COMPATIBLE> (1) :
```

Note: This prompt appears only if RIP is turned on.

6 Enter the version of RIP that you are using.

The default value is `compatible`. If you choose version 2, this means that the entire route, including the subnet mask, appears in the RIP packet. You should choose `compatible` if there are parts of your network that do not support RIP V2.

You have now created a new association for this interface.

Adding an association: an alternate method

Alternatively, you can enter the entire association on the command line as follows:

```
ip isdn2 association add 90.008.004.005
manufacturing enabled
```

Note: The entire command is entered on one line.

When you press <Enter>, you see

```
IP association added:

Internet address     :  90.008.004.005
Network              :  90.000.000.000
Circuit name         : manufacturing
IP                   : enabled
RIP mode             : off
RIP version          : compatible
```

Changing an association for an interface

To change an association for an interface, enter `ip isdn2 association change`.

See “Adding an association” for descriptions of prompts.

Deleting an association

To delete an existing association, enter `ip isdn2 association delete`.

The router prompts for the circuit name of the association you want to delete and then displays the entry.

```
Circuit Name <Up to 15 Characters or *> : energis

   Internet address : unnumbered
   Network          : <not assigned>
   Circuit name     : Energis
   IP               : enabled
   RIP mode         : standard
   RIP version      : compatible

Delete IP association <YES or NO> : no
```

The router does not delete the entry until you confirm that you want to do so.

Displaying the association table

To display the association table for an interface, enter `ip isdn2 association show.`

The following display appears:

```
IP Association Table
Node Address   Circuit Name    IP      RIP mode  Version   Warn
57.008.004.005 manufacturing enabled  standard  1         6
```

For more detailed information about a particular entry, including warnings, enter the IP address on the command line:

```
ip isdn2 association show 88.0.0.2
```

IP interface sub-context commands
association (as) (continued)

When you press <Enter>, you see

```
Internet address        :  90.008.004.005
   Network              :  90.000.000.000
   Circuit name         : manufacturing
   IP                   : enabled
   RIP mode             : active
   RIP version          : 1

WARNING  6 : Interface is disabled
WARNING 13 : Circuit is disabled
```

IP interface sub-context commands

circuit (ci)

Command purpose

The `ip isdn2 circuit` command is available on the ISDN interface. It lets you relate a circuit and an IP address using the circuit name.

> ***Note:*** The circuit command and the association table are different ways of accessing the same information.

Command syntax

The syntax of the `circuit` command is as follows:

```
HomeOffice: ip isdn2 circuit [show]
```

Using the command

Associating a circuit

1 To relate a circuit and an IP address, enter

`ip isdn2 circuit`

The router prompts as follows:

```
Circuit Name <Up to 15 Characters or *> :
```

2 Enter the name of the circuit and press <Enter>.

The router prompts you for an IP address.

```
Internet address <b1.b2.b3.b4 or unnumbered >:
```

This is the IP address to which you are linking the circuit.

3 Enter it and press <Enter>.

You see the following prompt:

```
IP <ENABLED or DISABLED> (enabled) : disabled
```

4 Define if IP is to be enabled on this circuit and press <Enter>.

You see the following prompt:

```
RIP Mode <STANDARD, TRIGGERED, DELTA, or OFF> (off)
:
```

5 Define which RIP mode you require on this circuit and press <Enter>.

The new association, with all of its attributes appears:

IP interface sub-context commands
circuit (ci) (continued)

```
IP association updated:

  Circuit name     : admin1
  Network          : 90.000.000.02
  Internet address : 90.000.000.01
  IP               : disabled
  RIP mode         : off
  RIP version      : compatible
```

Displaying the circuit table

To display the IP Circuit Table, enter `ip isdn2 circuit show` and press <Enter>.

The display appears as follows:

```
IP Association Table

Circuit Name   Node Address    IP         RIP Mode   Warning
admin1         90.000.000.02   disabled   off           -
manufacturing  88.000.000.002  enabled    triggered     -
personnel      88.000.000.003  enabled    off           -
```

To display a particular entry in more detail, including warnings, enter the circuit name on the command line and press <Enter>.

```
ip isdn2 circuit show admin1
```

The following appears:

```
Circuit name     : admin1      Network   : 90.000.000.01
Internet address : unnumbered  IP      : enabled
RIP mode         : off
RIP version      : compatible
```

IP interface sub-context commands

diat (d)

Command purpose

The `ip <interface> diat` command is available on the ISDN and Ethernet interfaces. It configures Dynamic IP Address Translation (DIAT) for single-host or multi-host use on a specified circuit. On the ISDN interface, it also enables and disables Dynamic IP Address Translation.

> ***Note:*** The HomeOffice Router must be using unnumbered links when configured to use DIAT.

DIAT is enabled by default.

Command syntax

The syntax of the `diat` command is as follows:

```
HomeOffice: ip eth1 diat

HomeOffice: ip isdn2 diat
```

Using the command

Configuring DIAT on an ISDN interface

1 To configure DIAT on an ISDN circuit, enter the following and press <Enter>.

```
ip isdn2 diat
```

The router responds as follows:

```
Circuit name <up to 15 Characters or *> :
```

2 Type the name of the circuit for which you want to change the DIAT parameters.

Note: The change does not take effect until you restart the router.

The router responds as follows:

```
DIAT mode <DISABLED, SINGLEHOST or
MULTIHOST> (multihost) :
```

Your response lets your router know whether you have one or more devices on your LAN.

IP interface sub-context commands
diat (d) (continued)

3 Select `SINGLEHOST` if you are connecting one device (for example, a PC) to your LAN.

Select `MULTIHOST` if you are connecting more than one device.

When you have made your selection, the changed configuration appears.

```
Circuit updated:

Circuit Name         : default
DIAT Mode            : singlehost
```

Configuring DIAT on an Ethernet interface

The HomeOffice Router supports a local Service Host Table that allows applications and users to connect to services (for example, WEB and mail services) on the router's LAN. The HomeOffice Router can be 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 router can forward this request to the correct device on the LAN. This allows local services to be exported without the remote site having to know the local IP address.

1 To configure DIAT on an Ethernet interface, enter the following and press <Enter>.

```
ip eth1 diat
```

The router responds as follows:

```
Service port number <1 - 65535 or
DEFAULT> (default) :
```

2 Type the TCP Port number of the service you want to select.

The router responds as follows:

```
New IP address <4 bytes b1.b2.b3.b4 or
NONE> ( 40.004.004.004) :
```

IP interface sub-context commands
diat (d) (continued)

3 Type the destination IP address to which you want to direct these service requests.

This updates the DIAT Service Host Table. Information similar to the following appears:

```
DIAT Service Host Table updated:

Service port number : 23
Host IP Address     :  70.004.004.004
```

IP interface sub-context commands

enabled (e)

Command purpose

The `ip <interface> enabled` command is available on all interfaces. It lets you enable and disable IP routing on each logical interface, and works identically on each interface.

Command syntax

The syntax of the `enabled` command is as follows:

```
HomeOffice: ip eth1 enabled [show]

HomeOffice: ip isdn2 enabled [show]
```

Using the command

Enabling IP on an interface

1 To enable IP routing, type the following and press <Enter>.

```
ip <interface> enabled
```

The router responds as follows:

```
Enable IP on interface <YES or NO> (yes) :
```

2 Enter `yes` if you want IP to be enabled on this interface, or `no` if you want to disable it.

The change does not take effect until you restart the router.

Note: You cannot enable IP on an interface if the interface does not have an IP address. If you have not already set an IP address on an interface, you see the following warning when you try to use this command:

```
An IP address has not been assigned to this
interface yet.
```

The router prompts you to select which IP address you want to enable.

```
Logical IP Interface Address <4 bytes b1.b2.b3.b4
or *> ( 70.001.001.000) :
```

Enter an asterisk (*) to list all the remote addresses on the physical interface that you are changing.

IP interface sub-context commands
enabled (e) (continued)

Displaying IP addresses for interfaces

This displays a table showing information for the logical IP interface addresses for all interfaces. For example, if you enter

```
ip eth1 enabled show
```

the following display appears:

```
IP Protocol Table

Interface             Enabled        Current
    70.001.001.000        yes          enabled
    10.001.001.000        yes          enabled
    11.001.001.000        yes          disabled
    20.001.001.000        yes          enabled
    22.001.001.000        yes          enabled
    24.001.001.000        yes          enabled
    23.001.001.000        yes          enabled
   127.000.000.001        yes          enabled
    89.000.003.203        yes          enabled
```

IP interface sub-context commands

icmp (i)

Command purpose

The `ip <interface> icmp` command is available on all interfaces and works identically on each of them. This command lets you define what the router does with Internet Control Message Protocol (ICMP) redirect messages on each logical interface.

ICMP provides information about why IP packets fail to get to their destinations.

Command syntax

The syntax of the `icmp` command is as follows:

```
HomeOffice: ip eth1 icmp [show]

HomeOffice: ip isdn2 icmp [show]
```

Using the command

Defining how ICMP redirect messages are handled

To define how ICMP redirect messages are handled by the HomeOffice Router, enter `ip <interface> icmp`.

If an IP address has been assigned to this interface, you see the following prompt:

```
Transmit ICMP redirects <ON or OFF> (off) :
```

You may want to stop the router from sending ICMP redirects on a WAN interface to save bandwidth. This should not be necessary on a LAN interface.

```
Listen for ICMP redirects <ON or OFF> (off) :
```

If you select `off`, the router ignores incoming ICMP redirects and does not use information provided by ICMP to update its Routing table. If you are running RIP (see the `rip` command on page 5-47), the router automatically ignores ICMP redirects.

IP interface sub-context commands
icmp (i) (continued)

When you have changed the ICMP parameters, you see

```
ICMP redirects updated:

    Interface                    : eth1
    Transmit ICMP redirects      : yes
    Listen ICMP redirects        : no
```

Note: If you have not already set an IP address on an interface, you see the following warning when you try to use this command.

```
An IP address has not been assigned to this
interface yet.
```

Displaying ICMP settings

To display the current settings for ICMP on each logical interface, enter `ip <interface> icmp show`.

A display similar to the following appears:

```
ip eth1 icmp show
                      ICMP Redirects
  Interface          Transmit       Listen
=>89.100.100.100       on             off
=>11.001.001.000       on             off
ip eth1
```

IP interface sub-context commands

lookup (l)

Command purpose

The `ip isdn2 lookup` command displays the last 20 lookup failures recorded in the association table. This information is useful if you are having trouble communicating with a particular destination.

Command syntax

The syntax of the `lookup` command is as follows:

```
HomeOffice: ip isdn2 lookup
```

Using the command

To display lookup failures, enter `ip isdn2 lookup`.

A display similar to the following appears:

```
IP Association Lookup Failures

Next hop router  Circuit   Fails   Last fail  Reason
                 -         5       7d 0h      Circuit not defined
router.91        paris     10      1d 12h     IP disabled on circuit
router.43        berlin    1       10m 1s     Circuit disabled
```

Parameter	Description
`Fails`	Tells you how many association lookups have failed for this circuit.
`Last fail`	Tells you how long ago the last failure occurred.

IP interface sub-context commands

relay (re)

Command purpose

The `ip eth1 relay` command is used to create a table of destinations for broadcasts that are routed off that network to remote destinations.

> ***Note:*** The `relay` command applies to all logical IP addresses on a physical Ethernet interface. However, the address you choose is the IP address of the physical interface, not the IP address of one of the logical interfaces on that physical interface.

Command syntax

The syntax of the command is as follows:

```
HomeOffice: ip eth1 relay <action>
```

where `<action>` is either `add`, `change`, `delete`, `enable`, or `show`.

Using the command

Note: If you have not already set an IP address on an interface, you see the following warning when you try to use this command.

```
An IP address has not been assigned to this
interface yet.
IP relay address table <ADD, CHANGE, DELETE, SHOW
or ENABLE> :
```

Enter the `enable` command if you want to use the IP addresses of NetBIOS or BootP devices. You see the following prompt:

```
Use IP relay addresses <ON or OFF> (off) :
```

This change will take effect the next time the unit is restarted using `top boot`.

IP interface sub-context commands
relay (re) (continued)

Creating a table of destinations

1 To create a table of destinations on an interface, type the following and press <Enter>:

```
ip eth1 relay add
```

The router responds as follows:

```
IP address <4 bytes b1.b2.b3.b4> :
```

2 Enter the IP address of the NetBIOS or BootP/DHCP server on which you want to receive broadcasts, or the broadcast address of the network on which the server is located.

You would most likely use the broadcast address if there are several servers on one network.

The router responds as follows:

```
Forward all UDP broadcasts <ON or OFF> (off) :
```

3 Do the following:

If you want to	Then
forward all types of UDP broadcasts, including NetBIOS and BootP/DHCP	type `on`. ***Note:*** Configuring `Forward all UDP broadcasts` to `ON` may keep your WAN links open unnecessarily.

forward only NetBIOS and/or BootP/DHCP packets	type `off`.
	The router prompts you for the following:
	`Forward NetBIOS packets <ON or OFF> (off) :`
	`Forward BOOTP/DHCP packets <ON or OFF> (off) :`
	Enable forwarding of NetBIOS and/or BOOTP/DHCP packets, as required.

IP interface sub-context commands
relay (re) (continued)

The router then confirms the details of the relay address that you added.

```
Relay address added:

Address                        :  85.0.0.2
   Forward all UDP broadcasts  : off
   Forward NetBIOS packets     : on
   Forward BOOTP/DHCP packets   : on
```

Note: The maximum number of entries in the Relay Forwarding Table is 16 per interface.

Changing destination details

The `ip eth1 relay change` command allows you to change the details of an existing relay address.

```
Relay address <IP address or *> :
```

Enter the address that you want to change. The prompts are then the same as for `relay add`.

Deleting destinations

The `ip eth1 relay delete` allows you to delete relay addresses.

Enter the address that you want to delete. The router displays details of the address and asks you for confirmation before deleting it.

```
Delete relay address <YES or NO> :
```

Displaying relay address details

This command displays details of the IP Relay Addresses to which packets are routed from bridge-only interfaces.

```
IP Relay Addresses

IP Address              Protocols
7.007.007.007           NetBIOS, BOOTP/DHCP
88.000.000.002          NetBIOS
```

IP interface sub-context commands

rip (ri)

Command purpose

The `ip <interface> rip` command allows you to enable and disable Routing Information Protocol (RIP) use on each logical interface. RIP is the dynamic routing protocol used on TCP/IP networks. For instance, you may decide not to run RIP on a WAN interface, to reduce WAN costs. However, you will probably want to keep RIP running on the LAN interface(s).

This command is available on all interfaces, and operates identically on each of them.

Command syntax

The syntax of the command is as follows:

```
HomeOffice: ip eth1 rip

HomeOffice: ip isdn2 rip
```

Using the command

Enabling RIP on an interface

1 To enable RIP on an interface, type the following and press <Enter>:

```
ip <interface> rip
```

If you have not already set an IP address on an interface, you see the following warning when you try to use this command.

```
An IP address has not been assigned to this
interface yet.
```

Use the address command to allocate an IP address to an interface.

The router responds as follows:

```
RIP <ON or OFF> (off) :
```

2 To enable RIP, type on.

The router responds as follows:

```
Interface cost <1 -15 or INFINITY> (1) :
```

The Interface Cost is the notional cost of using this interface. If there are several routes to a destination, the router chooses the one with the lowest interface cost.

3 Enter a value between `1` and `15`, or enter `infinity`.

If	Then
an interface gives access to a particularly expensive WAN	you may want to set the parameter quite high.
you want to force traffic to use a particular route	set the value quite low.

The router responds with the following (on an ISDN interface only):

```
Triggered Retry Count <0 - 99 or INFINITY> (5) :
```

4 Define the number of times that RIP tries to connect with RIP on the destination router, if they cannot communicate (for example, if communications fail).

The router responds with the following (on an ISDN interface only):

```
Triggered Retry Interval in minutes <1 - 10> (1) :
```

5 Define the time interval between triggered retry attempts.

The router responds as follows:

```
Include default routes in RIP packets
<YES or NO> (yes):
```

6 Include default routes in RIP packets, if required.

These are the routes defined using the `ip general route` command (see page 5-19).

The router responds as follows:

```
Ignore incoming RIP updates <YES or NO> (yes) :
```

Other network devices may send out RIP packets to exchange routing and service information. These packets can saturate the router's routing table.

IP interface sub-context commands
rip (ri) (continued)

7 Respond with `yes` or `no` as required.

If you choose to ignore these packets, you should set up a default or static route from the router using the `ip general route add` command.

The router responds with the following (on an Ethernet interface only):

```
RIP Version <1, 2 or COMPATIBLE> (compatible) :
```

8 Enter the version of RIP that you are using.

The default value is `compatible`. If you choose version 2, this means that the entire route, including the subnet mask, appears in the RIP packet.

You should choose `compatible` if there are parts of your network that do not support RIP V2.

Details of the new RIP settings appear. The screen will look something like this:

```
Routing Information Protocol updated:

  Interface                : isdn2
  RIP                      : on (current = off)
  Cost                     : 1
  Triggered Retry Count    : 5
  Triggered Retry Interval : 2 (current=1)
  Include default routes   : yes
  Ignore RIP Updates       : no
```

This change will take effect the next time the unit is "software restarted" using `top boot`.

Displaying RIP status

To display RIP status, enter `ip isdn2 rip show.`

This command displays the status of RIP on all of the router's interfaces similar to the following, with the arrow pointing to the current interface.

IP interface sub-context commands
rip (ri) (continued)

```
Routing Information Protocol

  Interface       RIP     Cost  Retry   Retry      Include        Warn
                                Count   Interval   Default Routes

=>89.100.100.100  on      1      -       -          yes            -
  9.039.049.000   off     1      1       5          yes            -
```

IP interface sub-context commands

spoof (sp)

Command purpose

The `ip eth1 spoof` command allows you to enable and disable spoofing of certain protocol data packets that are sent periodically by a LAN host to determine whether other parties are still connected. Without spoofing, these data packets would be rerouted over ISDN, incurring extra call charges unnecessarily. Spoofing means that the HomeOffice Router automatically responds to these packets without ever sending them over ISDN.

Command syntax

The syntax of the command is as follows:

```
HomeOffice: ip eth1 spoof
```

Using the command

1 To enable spoofing, enter `ip eth1 spoof`.

The router responds as follows:

```
Enable TCP keepalive spoofing <ENABLED or DISABLED>
(disabled)
```

2 Select `ENABLED` if required.

The router responds as follows:

```
Enable NetBIOS/IP keepalive spoofing <ENABLED or
DISABLED> (disabled)
```

3 Select `ENABLED` if required.

The spoofing status similar to the following appears:

```
Spoofing enable(s) updated.

  TCP          Spoofing status    :  enabled
  TCP NetBIOS  Spoofing status     :  enabled

This change will take effect the next time the unit
is “software restarted” using “top boot”.
```

IP filter sub-context commands

The commands in this sub-context let you configure and manipulate the protocol filtering commands.

In the `IP filter` sub-context, the command prompt is

```
HomeOffice: ip filter
```

The following commands are described in this section:

Command	Shortcut	Description
attachments	a	Attaches, detaches, and shows filters and interfaces or circuits.
copy	co	Copies an existing filter to another with a new name.
create	cr	Creates a new filter.
display	d	Shows all the currently defined elements for a given filter.
edit	e	Edits the contents of an existing filter.
remove	r	Deletes an existing filter.
test	te	Allows the testing of a filter by generating a packet that can be passed through the filter.

To display a list of available commands, enter `help`. To display a list similar to the one above, enter `help all`. To exit back to non-privileged level, enter `quit`.

CAUTION
Risk of loss of association
Protocol filtering is a complicated feature to set up. If you make a mistake, you may prevent any traffic from being forwarded, or cut off your remote administration session. Make sure you understand how it works before using it.

Note: For more information on protocol filtering, we recommend that you read a good reference book on network security, such as *Firewalls & Internet Security* by William Cheswick & Steven Bellovin, published by Addison-Wesley, ISBN number 0-201-63357-4.

IP filter sub-context commands

attachments (a)

Command purpose

The `IP filter attachments` command lets you attach or detach filters from interfaces or circuits. It also lets you show the current attachments.

Command syntax

The syntax of the `attachments` command is as follows:

```
HomeOffice: ip filter attachments <action>
```

where `<action>` is either `add`, `delete`, or `show`.

Using the command

Adding filter attachments

1 To add filter attachments, enter `ip filter attachments add`.

The router prompts you for the name of the filter that you want to attach to the specified interface or circuit.

```
Filter name <up to 15 Characters or *> :
```

2 Enter the filter name.

The router prompts you for the interface to which the filter should be added.

```
Interface name <up to 15 Characters or *> :
```

3 Enter the name of the interface on which you want the filter to operate.

If the interface has circuits, the router prompts you for the circuit name.

```
Circuit name <up to 15 Characters or *> :
```

4 Enter the circuit name.

The router asks whether the filter should be used on the input or output data of the interface or circuit.

```
Direction to attach filter <input or output> :
```

IP filter sub-context commands
attachments (a) (continued)

5 Enter `input` or `output` as required.

The router confirms that the attachment has been successful.

```
Successfully attached filter trialf to circuit
isdn2 on interface address 89.100.100.100
```

Deleting filter attachments

This command deletes an attachment between a specified filter and an interface or circuit.

1 To delete filter attachments, enter `ip filter attachments delete`.

The router prompts you for the number of the attachment you wish to delete.

```
Delete attachment number <number or *> :
```

2 Enter the attachment number and press <Enter>.

The router confirms that the attachment has been deleted.

```
Successfully detached filter
```

Displaying filter attachments

The `attachments show` parameter lets you view a list of all the currently defined attachments. The attachments are shown in the order in which they were entered:

Enter `ip filter attachments show`.

A display similar to the following appears:

```
Filter name   Interface/Circuit      Input/Output
1. trialf      89.100.100.100/isdn2   Output
```

IP filter sub-context commands

copy (co)

Command purpose

The `ip filter copy` command lets you copy an existing filter to another with a new name. The original filter is not altered. If you do not enter the name of either the source or destination filter, you are prompted for one.

Command syntax

The syntax of the `copy` command is as follows:

```
HomeOffice: ip filter copy
```

Using the command

1 To copy a filter, enter `ip filter copy.`

The router prompts you for a source filter.

```
Copy from filter name <Up to 15 Characters or *>:
```

2 Enter the name of the filter you want to copy.

The router prompts you for a destination filter.

```
Copy to filter name <Up to 15 Characters> :
```

3 Enter the name of the new filter.

The router confirms that copying is successful.

```
Filter main_1 copied to network_3
```

IP filter sub-context commands

create (cr)

Command purpose

The `ip filter create` command lets you define a filter and its component elements.

Command syntax

The syntax of the `create` command is as follows:

```
HomeOffice: ip filter create
```

Using the command

1 To create an IP filter, type the following and press <Enter>.

```
ip filter create
```

The router responds as follows:

```
Create filter name <up to 15 Characters> :
```

2 Enter a meaningful name for the filter you are about to create.

The router responds as follows:

```
Default element type <PERMIT or DENY> :
```

3 Type `permit` or `deny` and press <Enter>.

Selecting `permit` means that a packet that has passed through any of the previous filter elements is forwarded.

Selecting `deny` means the packet is not forwarded.

The router responds as follows:

```
New filter created.

Add an element <YES or NO> (yes) :
```

The default element is always the final element in the list of filter elements. It acts on any packets that do not match any of the filter's normal or include filter elements. If a packet has passed through any previously defined elements, the default element either permits or denies the packet.

4 Enter `YES` to enter an element.

The router responds as follows:

```
Position to insert <number, FIRST or LAST> (LAST) :
```

IP filter sub-context commands
create (cr) (continued)

This is the position in the filter list of elements. When the router is filtering, a packet is checked against each of the filter elements in the order of their position. The LAST position is the last normal or include filter element; the default element is always placed after these elements.

5 Respond as required.

The router responds as follows:

```
Insert filter or element <FILTER or ELEMENT>
(Element):
```

6 Enter a filter or element name.

Filter elements can be descriptions of permit or deny conditions, or the name of another existing filter. If the element is an included filter, then, during packet filtering, all the elements in that filter are checked.

Note: There are two types of elements other than the default element. These are called `normal` and `include filter`. `Include filter` elements are pointers to other filters. The `other` filters must exist before an `include filter` element that names them can be created.

If you include another filter, the default element of the included filter is not used.

The router responds as follows:

```
Source IP address <4 bytes b1.b2.b3.b4 or
ANY> (ANY) :
```

7 Enter the source IP address.

The router responds as follows:

```
Destination IP address <4 bytes b1.b2.b3.b4 or
ANY> (ANY) :
```

8 Enter the destination IP address.

The router responds as follows:

```
Protocol <ICMP, TCP, UDP or ALL> (All) :
```

9 Select the protocols you need to filter.

If you select `TCP` *the router prompts you for the following:*

```
TCP connection type <NEW or ANY> (any) :
```

IP filter sub-context commands
create (cr) (continued)

TCP packets contain a set of control flags used to determine the purpose and contents of these packets. One of these flags (the SYN flag) is used to initiate the synchronization of packet sequence numbers during the establishment of TCP connections. It is useful to be able to specify whether packets with this flag enabled are permitted or denied. Therefore, you can now set a filter that either acts on TCP packets with the SYN flag enabled, or that act on any TCP packets.

10 Do the following:

If you want	Then
a filter to act only on TCP packets with the SYN flag enabled	select NEW**.**
a filter to act on any TCP packets	select ANY**.**

Note: The default is ANY.

The router prompts you for the Element Type:

```
Element type <PERMIT or DENY> (deny) :
```

11 Respond as required.

The definition of the filter element is confirmed.

```
Filter element inserted.
```

The router prompts as follows:

```
Add an element <YES or NO> (yes) :
```

The router prompts you repeatedly to add elements until you type no*.*

12 Type yes or no as required.

The filter you added appears in the filter display format.

```
IP Filter   trialf3
Filter Attachments : No Attachments
Filter Elements :
Source       Destination  Protocol Source  Dest  Con   Type
Address/Mask Address/Mask          Port    Port

1. any       any           TCP     all     all   new   deny
   host      host
2. ---------------- Default element -----------         deny
```

IP filter sub-context commands
create (cr) (continued)

If you attempt to add more filters or elements than your router's memory is capable of supporting, the following message appears indicating the filter table is full:

```
No space left in filter table.
New element not added.
```

To add another filter or element, you must delete a filter or element.

Note: The `TCP connection type` prompt also appears in the `edit` command.

IP filter sub-context commands

display (d)

Command purpose

The `ip filter display` command shows all the currently defined elements and attachments for a specified filter. If you do not enter a filter name on the command line you are prompted to do so.

Command syntax

The syntax of the `display` command is as follows:

```
HomeOffice: ip filter display
```

Using the command

1 To display defined elements and attachments for a filter, type the following and press <Enter>.

```
ip filter display
```

The router responds as follows:

```
Filter Name <Up to 15 Characters, ALL or *>:
```

2 Enter a filter name.

The filter attachments and elements for the specified filter similar to the following appear:

```
IP Filter   trialf1

Filter Attachments :
 No Attachments

Filter Elements :
Source       Destination  Protocol  Source  Dest  Con  Type
Address/Mask Address/Mask             Port  Port

1  any          any          TCP    all   all   new  deny
   host         host
2 -------------- Default element -------------------- deny
```

IP filter sub-context commands

edit (e)

Command purpose

The `ip filter edit` command allows you to edit the contents of an existing filter.

Command syntax

The syntax of the `edit` command is as follows:

```
HomeOffice: ip filter edit
```

Using the command

1 To edit the contents of an existing filter, type the following and press <Enter>.

```
ip filter edit
```

The router responds as follows:

```
Filter Name <Up to 15 Characters or *> :
```

2 Enter the name of the filter you want to edit.

The router prompts you for an editing action.

```
Editing action <CHANGE, INSERT, DELETE, MOVE> :
```

See the relevant section below.

Changing filter contents

1 To edit the contents of existing elements, enter `change`.

The router prompts you for the number of the element you wish to edit.

```
Change element number <number or *> :
```

2 Type the element number and press <Enter>.

Note: Entering * at this prompt produces a display of the existing filter elements. If there are no elements currently defined, only the default element is shown.

If the selected element contains an included filter, the router prompts you to change the name for that included filter. For example:

```
Included Filter Name <Up to 15 Characters or
*> (old_name) :
```

IP filter sub-context commands
edit (e) (continued)

The existing name appears in parentheses and will be retained unless a new name is entered. The router checks that any entered name is a valid filter. A filter cannot include itself. Checks are made for endless loops. For example, where filter one includes filter two, which includes filter one, and so on.

If the selected element is a normal element, the router prompts you for each item in the element.

```
Source IP address <4 bytes b1.b2.b3.b4 or ALL>
(134.191.000.000) :
```

```
Destination IP address <4 bytes b1.b2.b3.b4 or ALL
> (ALL) :
```

```
Destination IP address mask <4 bytes b1.b2.b3.b4 or
HOST > (HOST):
```

```
Protocol <ICMP, TCP, UDP or ALL> ( ALL) :
```

Note: If the element has its protocol field set to `TCP` or `UDP`, you are prompted for a source and destination port range. Valid ranges are a number qualified with the less than sign (<), the greater than sign (>), or (!)(not). For example, `<24, >1024, !23` or a range such as `23 - 1023`.

If you selected `TCP` at the `Protocol` prompt above, the router prompts you to specify the `TCP` connection type.

3 Select `NEW` if you want a filter to act only on TCP packets with the SYN flag enabled. Select `ANY` if you want the filter to act on any TCP packets. The default is `ANY`.

The router prompts you for the element type.

```
Element type <PERMIT or DENY> (permit) :
```

Note: The router prompts you for each item in the element.

If you choose to edit the default element, the only parameters you can edit are the `permit` and `deny` parameters for each direction. For example:

```
DEFAULT element type <PERMIT, DENY> (permit) :
```

IP filter sub-context commands
edit (e) (continued)

Inserting a filter

1 To create a new filter element to be added to the filter currently being edited, type `insert` and press <Enter>.

The new element can be a normal element or the name of an included filter. You cannot insert another default element.

The router responds as follows:

```
Position to insert <number, FIRST or LAST> :
```

2 Enter the position where you want to add the new filter or element.

This is the position in the filter list of elements. When the router is filtering, a packet is checked against each of the filter elements in the order of their position. The LAST position is the last `normal` or `include filter` element; the default element is always placed after these elements.

Further prompts are the same as for the `filter create` prompts. Follow the `create` command to complete the insertion of a filter.

Deleting a filter element

Note 1: The delete option does not allow you to delete a filter. It allows you to delete only filter elements. To delete a filter, use the `remove` command (on page 5-66) to remove a filter.

Note 2: You cannot delete the default element.

1 To delete an existing element from the filter list, type `delete` and press <Enter>.

The router responds as follows:

```
Delete element number <number or *> :
```

2 Enter the number of the element you wish to delete.

Entering * displays all the existing filter elements.

IP filter sub-context commands
edit (e) (continued)

Moving an element to another position in the filter access list

1 To move an existing element to a different position in the filter access list, type `move` and press <Enter>.

The router prompts you for the number of the element you need to move.

```
Move element from number <number or *> :
```

2 Enter the element number you need to move.

Entering * displays all the existing filter elements.

The router prompts you for a new position for that element.

```
Move element to number <number or *> :
```

3 Enter the new position in the sequence where you want the element to operate.

IP filter sub-context commands

remove (r)

Command purpose

The IP filter `remove` command removes an existing filter from the filter table.

Removing a filter also deletes any attachments that use this filter. Any elements in other filters that include the filter being removed are also deleted.

Command syntax

The syntax of the `remove` command is as follows:

```
HomeOffice: ip filter remove
```

Using the command

1 To remove a filter from the filter table, enter `ip filter remove`.

If you did not enter the name of the filter or interface with the command, the router prompts you to do so, as follows:

```
Remove filter name <up to 15 Characters or *> :
```

Note: Entering `*` at this prompt displays all the existing filters.

After specifying the filter name, you are asked to confirm the removal of the filter.

```
Confirm removal of filter <YES or NO> :
```

2 Enter `yes`.

This confirms removal of the filter as follows:

```
Filter <filter name> removed.
```

IP filter sub-context commands

test (te)

Command purpose

The `ip filter test` command lets you test the logic of the elements you have defined for a filter. It does this by generating a test packet that is passed through the filter.

Command syntax

The syntax of the `test` command is as follows:

```
HomeOffice: ip filter test
```

Using the command

1 To test element logic for a filter, type the following and press <Enter>.

```
ip filter test
```

The router responds as follows:

```
Filter name <up to 15 Characters or *> :
```

2 Enter the name of the filter you wish to test.

3 Respond to the following prompts.

Note: More information about these prompts can be found in the topic “create (cr)” on page 5-57.

```
Packet source IP address <4 bytes b1.b2.b3.b4> :
Packet destination IP address <4 bytes
b1.b2.b3.b4>:
Protocol <ICMP, TCP or UDP> :
Source port <number [14 chars]> :
Destination port <number [14 chars]> :
TCP connection type <NEW or ANY> (any) :
```

IP filter sub-context commands
test (te) (continued)

4 Enter the elements you want to include in the test packet.

The result of the test indicates whether the packet passed through the test filter. If the packet was denied, the information includes the filter element that stopped it.

For example, you receive the following message if the test packet did not match the first two filter elements and was then stopped by the third element.

```
packet denied by element 3
```

IPX context shell commands

The `ipx` context lets you manage IPX routing. Commands are grouped together into sub-contexts. The following sub-contexts are described, as examples:

Sub-context	Description
general	Configure IPX parameters that apply regardless of interface.
eth1	Configure IPX parameters specific to an Ethernet interface.
isdn2	Configure IPX parameters specific to an ISDN interface.

IPX general sub-context commands

The `ipx general` sub-context lets you manage those aspects of IPX routing that are not interface-dependent.

In the `IPX general` sub-context, the command prompt is

```
HomeOffice: ipx general
```

The following commands are described in this section:

Command	Shortcut	Description
address	ad	Sets up local IPX addressing information for bridging interfaces.
datalink	d	Specifies the data link layer for IPX to run over.
enabled	e	Enables or disables IPX on bridging interfaces.
filtersap	fs	Defines SAP filters.
forward	fo	Displays the dynamic Routing table.
rip	ri	Sets up the Routing Information Protocol (RIP) on bridging interfaces.
route	ro	Modifies the static Routing Table.
sap	sa	Sets up the Service Advertising Protocol (SAP) on bridging interfaces.
service	ser	Displays the dynamic, and modifies and displays the static Service tables.
statistics	ss	Displays IPX routing statistics.

To display a list of available commands, enter `help`. To quit back to non-privileged level, enter `quit`.

IPX general sub-context commands

address (ad)

Command purpose

The `ipx general address` command sets up local IPX addressing information for bridging-only interfaces.

Command syntax

The syntax of the `address` command is as follows:

```
HomeOffice: ipx general address
```

Using the command

To set up an address, enter `ipx general address`.

To display the current address, enter `ipx general address show`.

When you enter the `ipx general address` command, the router prompts for the following values:

```
Network <8 hex digits, name, * or NONE> (23456789):
```

This identifies the network to which the router is attached.

```
Number of ticks in 1/18th secs (1 - 65535) (1):
```

The number of ticks is a measure of the time necessary to deliver a 576-byte packet to a node on that network, in 1/18th 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)—probably never shorter than two seconds (36 ticks). If the line speed is 1200 baud, even that would be too quick. Probably five or ten times this value would be required.

```
Forward broadcasts to this interface
<YES or NO> (yes):
```

IPX general sub-context commands
address (ad) (continued)

This lets you specify whether or not you want broadcasts forwarded onto the LAN.

```
Forward NetBIOS packets to this interface
<YES or NO> (yes) :
```

This lets you specify whether or not to forward NetBIOS packets.

```
Forward Netware security packets to this interface
<YES or NO> (yes) :
```

Novell Servers that know about each other exchange security packets every 60 seconds. This can increase WAN costs considerably. The router does not normally forward these security packets. If you do want to forward these packets, enter `yes` at this prompt.

```
Spoof Watchdog packets received on this interface
<YES or NO> (yes) :
```

This lets you activate the use of 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 server, to maintain the connection. Since they are sent locally, the transmission costs are lower.

```
Spoof NetBIOS Probe packets received on this
interface <YES or NO> (yes) :
```

This lets you specify whether or not to spoof NetBIOS probe packets.

```
Spoof of SPX Probe packets received on this interface
<YES or NO> (yes) :
```

IPX general sub-context commands
address (ad) (continued)

This lets you enable 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. 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.

```
Version of SPX Spoofing <V1, V2 or PIGGYBACK> :
```

Choose the version of SPX spoofing you want to use. We recommend that you use `piggyback` as a default. You must use the same version at both ends of the link.

An update similar to the following appears:

```
IPX Bridge address updated

Network                       : 23456789
Number of ticks               : 1
Forward broadcasts            : yes
Forward NetBIOS packets       : yes
Forward security packets      : yes
Watchdog packet spoofing      : yes
SPX probe packet spoofing     : yes
SPX probe version             : piggyback
NetBIOS probe packet spoofing : no
```

Note: If you make changes to the network address(es), these only take effect after you restart the router. So when you have finished setting the addresses, enter `top boot`.

IPX general sub-context commands

datalink (d)

Command purpose

The `ipx general datalink` command lets you specify which IPX data link layer to use. In the `ipx general` context, it only applies to bridging interfaces.

Command syntax

The syntax of the `datalink` command is as follows:

```
HomeOffice: ipx general datalink [show]
```

Using the command

Specifying the data link layer to use

To specify which data link layer to use, enter `ipx general datalink`.

You see this prompt:

```
Datalink layer <ETHER2, 802.2, SNAP or
802.3> (802.2):
```

Select a data link layer to match the data link layer you have configured on your servers and workstations. The values are:

Layer	Description
ETHER2	IPX uses a unique packet header (type code). This value is suitable for networks that involve DEC or the TCP/IP protocol.
802.2	The router uses the IEEE and OSI standard 802.2 frame type. 802.2 is the default value.
SNAP	The router uses the IEEE and OSI standard 802.2 frame type with the 802.2 SNAP extension.
802.3	The router uses a standard Novell frame on a network that uses only NetWare.

IPX general sub-context commands
datalink (d) (continued)

Displaying the current datalink

To display which current layer is selected, enter `ipx general datalink show`.

The following appears:

```
Datalink layer : 802.3
```

IPX general sub-context commands

enabled (e)

Command purpose

The `ipx general enabled` command applies to bridging interfaces, and activates or deactivates IPX.

Command syntax

The syntax of the `enabled` command is as follows:

```
HomeOffice: ipx general enabled [show]
```

Using the command

Enabling IPX

To enable IPX, enter `ipx general enabled`.

The following prompt appears:

```
Enable IPX on bridged interfaces <YES or NO> (no) :
```

Enter `yes` if you want IPX to be enabled on bridging interfaces, or `no` if you want it to be disabled.

The change does not take effect until you restart the router.

Displaying interfaces on which IPX is enabled

To display a table showing the bridging interfaces on which IPX is enabled, enter `ipx general enabled show`.

The following appears:

```
IPX Protocol Table

Interface    Enabled     Current
       eth1          yes          enabled
       isdn2         yes          disabled
=>     bridge         yes          enabled
```

IPX general sub-context commands

filtersap (fs)

Command purpose

The `ipx general filtersap` command lets you add, change, delete, and show SAP filters.

Command syntax

The syntax of the `filtersap` command is as follows:

```
HomeOffice: ipx general filtersap <action>
```

where `<action>` is either `add`, `change`, `delete`, or `show`.

Using the command

To work with SAP filters, enter `ipx general filtersap.`

The router prompts you for an editing action.

```
SAP filter element <ADD, CHANGE, DELETE or SHOW> :
```

See the relevant section below.

Adding SAP filters

Select `add` if you want to add a SAP filter element.

```
Filter name <up to 15 Characters> :
```

Enter the name of the filter.

```
Filter direction <IN or OUT> (NONE) :
```

Specify the direction (incoming or outgoing) to which the filter applies.

```
Filter service type(s) <all !number, number or range
[14 chars]> (not assigned) :
```

Enter the number or range of IPX services that you do not want forwarded to other devices. Enter `all` if you do not want to forward information on any services.

An update similar to the following appears:

```
New filter added:
   Name           : trialf2
   Range          : 23
   Application    : BOTH
   Filter direction : IN
```

This change will take effect the next time the unit is "software restarted" using the `top boot` command.

Changing SAP filters

Select `change` if you want to change a SAP filter element.

```
Filter name <up to 15 characters or *>:
```

Enter the name of the filter whose SAP filter element you want to change.

```
Filter name <up to 15 characters or *>
(the_filter_name):
```

Enter the new name of the filter element.

```
Filter direction (IN or OUT) (IN):
```

Enter the new direction for the filter.

```
Filter service type(s) <number or range [14 chars]>
(23):
```

Enter the filter type range to suit your needs.

```
Filter interface application <LAN, WAN or BOTH> :
```

Choose whether you want this application to apply to the LAN or WAN, or both. You receive a confirmation that the filter has been updated.

IPX general sub-context commands
filtersap (fs) (continued)

```
   Name             : trialf2
   Range            : 23
   Application      : LAN
   Filter direction : OUT

Filter trialf2 updated.
```

Displaying SAP filters

Select `show` if you want to display a SAP filter element.

```
SAP Filter Table

Name      Range     Application   Filter direction
trialf2     all       LAN             OUT
```

Deleting SAP filters

Select `delete` if you want to delete a SAP filter element.

```
Filter name <up to 15 Characters> :
```

Enter the name of the filter whose SAP filter element you want to delete. You then see a summary of the filter you want to delete and a prompt asking you to confirm its deletion.

IPX general sub-context commands

forward (fo)

Command purpose

The `ipx general forward` command lets you check the information currently stored in the IPX forwarding table.

Command syntax

The syntax of the `forward` command is as follows:

```
HomeOffice: ipx general forward [destination address]
```

Using the command

To view the IPX forwarding table, enter `ipx general forward`.

The following information appears:.

```
                IPX Dynamic Route Table
Destination- NextHopNode  NextHopNetwork Ticks Hops Lifetime Alt
10000000     -            -                1    1   direct  0
12341234     10456456451 54654654          1    1   static  0
```

Column	Description
`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 1/18th of a second. If the destination is reached over the Ethernet interface, this is `1`. For WAN links, the time depends on line speed, and how busy the line is.
`Hops`	This is the number of routers that traffic passes through to reach the destination.
`Lifetime`	This is the length of time before the entry times out. In the example above, the entry is for one of the router's own interfaces. This is marked as `direct`. Entries made manually by a user are `static`.
—continued—	

IPX general sub-context commands
forward (fo) (continued)

Column	Description
`Alt`	This is the number of alternative routes available to the destination. You can only enter one route statically. Alternative routes are acquired dynamically.
—end—	

To see an individual entry and all the stored alternatives, enter `ipx general forward`, followed by the appropriate destination address. For example:

```
HomeOffice: ipx general forward 10000000
```

When you press <Enter>, information similar to the following appears:

```
Destination network : 10000000
Next hop node       : -
Next hop network    : -
Number of ticks     : 1
Number of hops      : 1
Lifetime            : directly connected
```

IPX general sub-context commands

rip (ri)

Command purpose

Routing Information Protocol (RIP) is the dynamic routing protocol used on IPX networks. The `ipx general rip` command (which only applies to interfaces used for bridging) enables and disables RIP for IPX.

Command syntax

The syntax of the `rip` command is as follows:

```
HomeOffice: ipx general rip [show]
```

Using the command

Enabling or disabling RIP

To enable IPX RIP, enter `ipx general rip`.

The router prompts:

```
RIP on bridged interfaces <ON or OFF> (on) :
```

Enter `on` if you normally want RIP to run, or `off` if you do not want it to run at all.

Displaying RIP status on interfaces

To display the status of RIP on all of the router's interfaces, enter `ipx general rip show`.

A screen similar to the following appears with the arrow pointing to the current interface:

```
    Routing Information Protocol

    Interface      RIP        Retry     Retry
                              Count     Interval
    eth1           on           -          -
    isdn2          off          5          1
=>  bridge         off          5          1
```

IPX general sub-context commands

route (ro)

Command purpose

The `ipx general route` command configures the static entries in the Routing table.

Command syntax

The syntax of the `route` command is as follows:

```
HomeOffice: ipx general route <action>
```

where `<action>` is either `add`, `change`, `delete`, `learn`, or `show`.

Using the command

Statically entered routing addresses are stored permanently in the router's Routing table, where they define the routes by which the router reaches remote networks. You can enter up to three static routes to any remote network. The `route` command lets you enter this information explicitly.

The Routing table also contains information provided by RIP and ICMP.

Adding routes

1 To enter a static route to the Routing table, enter `ipx general route add` and press <Enter>.

The following prompt appears:

```
Destination network <8 hex digits, DEFAULT, name or
*> :
```

2 Enter the name or address of the final destination network.

This must not be a network to which the router is directly connected.

The following prompts appear:

```
Next hop node <12 hex digits> :
Next hop network <8 hex digits> :
```

IPX general sub-context commands
route (ro) (continued)

3 Enter the node and network addresses 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 attached.

The following prompts appear:

```
Number of ticks in 1/18th secs <1 - 65535> (36) :
Number of hops <1 - 15> (2) :
```

4 Enter the ticks and hops it takes to reach the destination network.

The following table describes ticks and hops.

Term	Description
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 1/18th of a second. If the destination is reached over the Ethernet interface, set this to 1. For wide area links, the time depends upon the line speed and how busy the line is. Values should be conservative (that is, long)—probably never shorter than two seconds (36 ticks). If the line speed was 1200 baud, even that would be too quick. Probably five to ten times this value would be required. The number of ticks you enter should be the sum of the time needed to cross all of the networks on the route to the destination.
Hops	The number of hops is the number of routers that traffic must travel through to reach the destination.

Note: If two routes have the same number of ticks, the one with the smallest number of hops is used (that is, with the smallest number of routers). You can enter an artificially high or low number of ticks and hops to force the router to use (or not use) a particular route.

If two routes have identical names, the router uses the static route and ignores the dynamic route.

IPX general sub-context commands
route (ro) (continued)

Changing routes

To edit a static route, enter `ipx general route change`, followed by the address of the remote network or node.

If you are not sure what is in the Routing Table, enter `ipx general route change *` to list the possible node and network addresses.

The router prompts for the same values as for `route add`.

Enter a new value or press <Enter> to leave a value unchanged. If there is more than one entry for the node or network you specify, each entry appears in turn.

Deleting routes

To delete a static route from the Routing table, enter `ipx general route delete`, followed by the node or network address.

If you are not sure exactly what is in the Routing Table, enter `route delete *` to list the possible node or network addresses.

The router displays the entry and the following prompt:

```
Delete IPX route <YES or NO> :
```

Confirm the deletion by entering `yes`.

Storing dynamic routes as static routes

To store routes that have been entered manually (that is, dynamically) for future use, enter `ipx general route learn`.

The router looks for individual dynamic entries, and asks you to confirm that you want them to be stored as static entries.

IPX general sub-context commands
route (ro) (continued)

Displaying static routes

To display static routes, enter `ipx general route show`.

When you press <Enter>, you see

```
                    IPX Static Route Table
 Dest'n   Next hop        Next hop   Ticks  Hops  Warning
          node            network
 01111111 100000000000    00000001    1     2        -
```

To display an individual entry, including Warnings, enter `ipx general route show <destination>`.

Note: To display the entire Routing table, use the `forward` command.

IPX general sub-context commands

sap (sa)

Command purpose

The `ipx general sap` command lets you specify how the Service Advertising Protocol (SAP) is to operate on interfaces used for bridging. SAP provides devices on the network with information about which services are available from which devices.

Command syntax

The syntax of the `sap` command is as follows:

```
HomeOffice: ipx general sap [show]
```

Using the command

Configuring SAP

1 To reconfigure SAP, enter `ipx general sap`.

The following prompt appears:

```
SAP on bridged interfaces <ON or OFF> (on) :
```

2 Enter `on` if you want to enable SAP or `off` to disable SAP.

Displaying SAP status

To display the current state of SAP on all interfaces, enter `ipx general sap show`.

When you press <Enter>, you see

```
Service Advertising Protocol

    Interface      SAP         Retry     Retry
                               Count     Interval
    eth1           on              -           -
    bridge         on              5           1
=>  isdn2          off             5           1
```

IPX general sub-context commands

service (ser)

Command purpose

The Service table lists the services that the router can reach.

The `ipx general service` command configures the static entries in the Service table. You can also use it to display the dynamic entries in the Service table.

Information is also provided by SAP. Static entries are permanent and must be removed explicitly; they do not time out.

Command syntax

The syntax of the `service` command is as follows:

```
HomeOffice: ipx general service <action>
```

where `<action>` is either `add`, `change`, `delete`, `learn`, `dynamic`, or `show`.

Using the command

Adding static entries

1 To add a static entry to the Service table, enter `ipx general service add`.

The router prompts for the following information:

```
Name <up to 47 characters> :
```

2 Enter the name of the service.

It 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 cannot access the required service.

The following prompt appears:

```
Service type <0 - 65535> :
```

IPX general sub-context commands
service (ser) (continued)

This is a decimal value indicating the type of service provided. 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.

The Name and the Service type must form a unique pair.

3 Enter the service type.

The following prompt appears:

```
Node <12 hex digits, name or *> :
```

4 Enter the node address of the device where the service is found.

The following prompt appears:

```
Network <8 hex digits, name or *> :
```

5 Enter the address of the network on which the node is providing service.

The following prompt appears:

```
Socket <0 - 65535> :
```

6 Enter the socket identifying the service.

If you need to find out the socket number of a service, you can enter `service show <servicename>` on a router attached to the same LAN as the server providing the service.

The following prompt appears:

```
Number of hops <1 - 15> (2)
```

7 Enter the number of routers that traffic has to pass through in order to reach the destination network.

Normally a client 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.

When you have finished adding an entry, the router displays it.

```
IPX service added:

   Service name   : printing
   Service type   : 2
   Node           : 100000000001
   Network        : 10000001
   Socket         : 34
   Number of hops : 1
```

IPX general sub-context commands
service (ser) (continued)

Changing a service

To change an existing static entry, enter `ipx general service change`.

The prompts are the same as those shown for `service add`. At each prompt, you can either enter a new value or press <Enter> to keep the current value.

Deleting a service

To delete a static entry from the Service table, enter `ipx general service delete`, followed by the entry's name.

The router displays the entry and asks you to confirm that you want to delete it.

Storing dynamic entries as static entries (learning services)

To save manually entered (dynamic) entries as static entries, enter `ipx general service learn`.

These do not time out and are available until deleted.

Displaying dynamic (and static) entries

> ***Note:*** If you want to display only static service entries, use the `show` option.

To display both static and dynamic entries in the Service table, enter `ipx general service dynamic`.

All services learned dynamically by SAP as well as services added statically by the administrator appear as follows:

```
IPX Dynamic Service Table
Service    Type    Node             Network    Lifetime
printing    2      100000000001     10000001   static
```

IPX general sub-context commands
service (ser) (continued)

To display a particular entry in more detail, enter `ipx general service dynamic <name>`.

A display similar to the following appears:

```
ipx general service dynamic printing
   Service name   : printing
   Service type   : 2
   Node           : 100000000001
   Network        : 10000001
   Socket         : 34
   Number of hops : 1
   Lifetime       : static
```

Displaying static entries only

Note: If you want to display both dynamic and static entries, use the `dynamic` option.

To display only static entries in the Service table, enter `ipx general service show`.

You see

```
IPX Static Service Table
Service  Type  Node          Network    Warning
printing   2   100000000001  10000001      -
```

To display an individual entry, enter `ipx general service show`, followed by the service name.

IPX general sub-context commands
service (ser) (continued)

You see

```
IPX service entry:
   Service name   : printing
   Service type   : 2
   Node           : 100000000001
   Network        : 10000001
   Socket         : 34
   Number of hops : 1
```

IPX general sub-context commands

statistics (ss)

Command purpose

The `ipx general statistics` command displays information on IPX routing carried out by the router.

Command syntax

The syntax of the `statistics` command is as follows:

```
HomeOffice: ipx general statistics
```

Using the command

Error and dropped datagram totals should remain low. If they rise suddenly, this may indicate a problem with your network.

To display IPX routing statistics, enter `ipx general statistics`.

The display looks like this.

```
Total datagrams received :           0
  For applications       :           0 (  0.00%)
  For forwarding         :           0 (  0.00%)
  Discarded datagrams
    Header error           :         0 (  0.00%)
    Address error          :         0 (  0.00%)
    Protocol error         :         0 (  0.00%)
    Other error            :         0 (  0.00%)
Total datagrams sent     :       26175
  From applications      :       26175 (100.00%)
  Discarded datagrams
    Lack of route          :         0 (  0.00%)
    Other error             :         0 (  0.00%)
```

Error types are described in the following table.

IPX general sub-context commands
statistics (ss) (continued)

Error type	Description
Header error	There is an error in the format of the IPX header.
Address error	The IPX is invalid or unexpected.
Protocol error	The datagram is not an IPX datagram. This may indicate problems at the Application level.

IPX interface sub-context commands

The HomeOffice Router has a sub-context for each of its physical interfaces. The commands in these sub-contexts let you configure the specific interface to route IPX.

In the `IPX <interface>` sub-context, the command prompts are

```
HomeOffice: ipx eth1
```

```
HomeOffice: ipx isdn2
```

The following commands are described in this section:

Command	Shortcut	Interface	Description
address	ad	eth1 isdn2	Allocates this interface's Node and Network address.
association	as	isdn2	Relates a Node or Network address to a circuit using the circuit name (ISDN only).
circuit	ci	isdn2	Relates a circuit to a Node or Network address using the circuit name (ISDN only).
datalink	d	eth1 isdn2	Selects the data link layer to use on an interface (Ethernet only).
diat	di	isdn2	Configures single-host or multi-host Dynamic IPX Address Translation (DIAT).
enabled	e	eth1 isdn2	Enables or disables IPX routing on this interface.
lookup	l	isdn2	Displays information about failed IPX calls (ISDN only).

—continued—

Command	Shortcut	Interface	Description
rip	ri	eth1 isdn2	Enables or disables Routing Information Protocol (RIP) on this interface.
sap	sa	eth1 isdn2	Specifies how Service Advertising Protocol (SAP) is to operate on this interface.
—end—			

To display a list of available commands, enter `help`. To return to non-privileged level, enter `quit`.

IPX interface sub-context commands

address (ad)

Command purpose

The `ipx <interface> address` command is available in all contexts, and sets up node and network addresses for an interface.

Not all prompts appear on all interfaces.

Command syntax

The syntax of the `address` command is as follows:

```
HomeOffice: ipx eth1 address

HomeOffice: ipx isdn2 address
```

Using the command

1 To define node and/or network addresses for an interface, enter `ipx <interface> address`, where `<interface>` is either `eth1` or `isdn2`.

The router prompts for the following:

```
Node <12 hex digits, name or *> (not assigned) :
```

Note: This prompt does not appear on an Ethernet interface. On Ethernet interfaces the router uses its MAC address as its node address, and can detect it automatically.

2 On an ISDN interface, enter the node address.

The router prompts for the following:

```
Network <8 hex digits, name or *> (not assigned):
```

3 Enter the address of the network to which the router is attached.

The router prompts for the following:

```
Number of ticks in 1/18th secs <1 - 65535> (1) :
```

IPX interface sub-context commands
address (ad) (continued)

The number of ticks is a measure of the time necessary to deliver a 576-byte packet to a node on that network, in 1/18th of a second.

Values should be conservative (that is, long)—probably never shorter than two seconds (36 ticks). If the line speed is 1200 baud, even that would be too quick. Probably five or ten times this value would be required.

If the destination is reached over the Ethernet interface, set this to `1`.

For wide area links, the time depends upon the line speed and how busy the line is.

The router prompts for the following:

```
Forward broadcasts to this interface
<YES or NO> (yes):
```

4 Do the following:

For	Then
an Ethernet interface	specify if you want broadcasts forwarded onto the LAN or not.
an ISDN interface	set this to `ON` if you want to forward broadcasts onto the Ethernet interface.

The router prompts for the following:

```
Forward NetBIOS packets to this interface
<YES or NO> (yes) :
```

5 Specify whether or not to forward NetBIOS packets.

The router prompts for the following:

```
Forward Netware security packets to this interface
<YES or NO> (yes) :
```

Novell Servers that know about each other exchange security packets every 60 seconds. This can increase WAN costs considerably. By default, the router does not forward these security packets.

6 If you want to forward Netware security packets, enter `yes`.

The next prompt displayed depends on whether you are working with the Ethernet or ISDN interface.

If you are working with the Ethernet interface, see “Ethernet interface” on page 6-31. If you are working with the ISDN interface, see “ISDN interface” on page 6-33.

Ethernet interface

The router prompts for the following:

```
Spoof Watchdog packets received on this interface
<YES or NO> (yes) :
```

This lets you activate the use of 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 they are sent locally, the transmission costs are lower.

1 Do the following:

If you	Then
want to activate Watchdog spoofing	enter `yes`.
do not want to activate Watchdog spoofing	enter `no`.

The router prompts for the following:

```
Spoof NetBIOS Probe packets received on this
interface <YES or NO> (yes) :
```

2 Enter `yes` if you want to activate the use of NetBIOS probe spoofing; otherwise, enter `no`.

The router prompts for the following:

```
Spoof of SPX Probe packets received on this
interface <YES or NO> (yes) :
```

This lets you activate the use of SPX probe spoofing. Based on a similar principle to Watchdog spoofing, SPX Spoofing significantly reduces network costs because probe packets are responded to locally by the router and are not sent across the WAN link. In general, you should enable SPX probe spoofing over a synchronous interface only if you are running boundary routing.

IPX interface sub-context commands
address (ad) (continued)

When you enable spoofing on an Ethernet interface, this spoofs packets received that are destined for WAN interfaces. It does not spoof packets destined for another Ethernet interface that has spoofing enabled.

3 Do the following:

If you	Then
want to activate SPX probe spoofing	enter `yes`.
do not want to activate SPX probe spoofing	enter `no`.

The router prompts for the following:

```
Version of SPX Spoofing <V1, V2 or PIGGYBACK> :
```

It is recommended that you use Piggyback spoofing of SPX Probe packets. This means that the packets are only spoofed when a call is not open and are passed as normal when a call is open. The same version must be used at both ends of the link.

4 Enter the SPX spoofing version.

The display similar to the following appears.

```
eth1 IPX address update:
   Network                       : 33333333
   Number of ticks               : 1
   Forward broadcasts            : yes
   Forward NetBIOS packets       : yes
   Forward security packets      : yes
   Watchdog packet spoofing      : yes
   SPX probe packet spoofing     : yes
   SPX probe version             : V1
   NetBIOS probe packet spoofing : yes

   IPX on this interface will be enabled.
```

Changes to node or network address(es) take effect only after you restart the router. So when you have finished setting the addresses, enter `quit`. When you are asked if you want to restart the router, type `y`.

IPX interface sub-context commands
address (ad) (continued)

ISDN interface

The router prompts for the following:

```
Route/service hold-down timer in minutes
<0-1440> (3):
```

This prompt does not appear on Ethernet interfaces.

When the router realizes that a circuit is not responding, it deletes all routes and services dependent on that circuit.

1 Enter the number of minutes that should elapse before all dependent routes and services are deleted.

Note: It is sometimes appropriate to set a value of less than three minutes, where a faster response to the failure of a circuit is required. This is only recommended if the unit 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; a value of three minutes is recommended and is suitable for most situations. Increasing this timer has the effect of reducing the number of network reconfigurations on networks that suffer short-term link failures. The network also takes longer to reconfigure when a permanent link failure occurs.

The display similar to the following appears.

```
isdn2 IPX address update:
   Node                          : 08003904C813
   Network                       : 32425456
   Number of ticks               : 36
   Forward broadcasts            : no
   Forward NetBIOS packets       : no
   Forward security packets      : no
   Route/service hold-down timer : 3
```

Changes to node or network address(es) take effect only after you restart the router. So when you have finished setting the addresses, enter `quit`. When you are asked if you want to restart the router, type `y`.

Displaying node and network addresses

To display the router's node and network addresses on each of its interfaces, enter, `ipx <interface> address show`.

IPX interface sub-context commands

association (as)

Command purpose

The `ipx isdn2 association` command lets you relate a node or network address to an ISDN circuit using its circuit name.

This command is not available in `Ethernet` sub-contexts.

Command syntax

The syntax of the `association` command is as follows:

```
HomeOffice: ipx isdn2 association <action>
```

where `<action>` is either `add`, `change`, `delete`, or `show`.

Using the command

To work with associations, enter `ipx isdn2 association`.

The router prompts you for an editing action.

```
association entry <ADD, CHANGE, DELETE or SHOW> :
```

See the relevant section below.

Creating new associations

1 To create a new association for this interface, enter `ipx isdn2 association add`.

The router prompts for the following information:

```
Node <12 hex digits>  :
```

2 Enter the node address of the destination you want to reach.

You do not need to enter the network address as the router can work this out.

Note: At this prompt, you can also enter * to list circuit names that can be associated with this interface. A circuit name is required for the next prompt.

The router prompts for the following information:

```
Circuit Name <Up to 15 Characters or *>:
```

IPX interface sub-context commands
association (as) (continued)

3 Enter a circuit name and press <Enter>.

The circuit must be accessible from this interface.

The router prompts for the following information:

```
IPX <ENABLED or DISABLED> (enabled) :
```

4 Enable or disable IPX.

The router prompts for the following information:

```
RIP mode <BROADCAST, TRIGGERED or OFF> (triggered):
```

5 Enable or disable RIP.

The router prompts for the following information:

```
SAP mode <BROADCAST, TRIGGERED or OFF> (triggered):
```

6 Enable or disable SAP.

When you have completed these parameters, you see

```
IPX association added:
  Node  : 100000000000  Network  : 10000000
  Circuit Name : admin         RIP  : off
```

Disabling IPX routing on a circuit

You can also use `association` to disable IPX routing on this circuit. You can enter the entire association on the command line, as follows:

```
ipx isdn2 association add 000000000001 personnel
enabled off off
```

When you press <Enter>, you see

```
IPX association added:

  Node         : 000000000001   Network : 10000000
  Circuit Name : personnel      RIP     : off
  IPX          : enabled        SAP      : off
```

IPX interface sub-context commands
association (as) (continued)

Changing associations

To change an existing association, enter `ipx isdn2 association change`.

The prompts are the same as for `association add`.

Deleting associations

1 To delete an association, enter `ipx isdn2 association delete`.

The router prompts for the node address.

```
Node <12 hex digits, name or *> :
```

2 Enter the node address and press <Enter>.

The router displays the association you want to delete and asks you to confirm deletion.

```
   Node         : 100000000000   Network   : 10000000
   Circuit Name : admin          RIP       : off
   IPX          : enabled        SAP       : off
Delete IPX association <YES or NO> :
```

The router does not delete the entry until you confirm that you want to do so.

3 To confirm the deletion, press <Enter>.

The following message appears:

```
IPX association to circuit admin deleted.
```

IPX interface sub-context commands
association (as) (continued)

Displaying associations

To display the IPX association table for the ISDN interface, enter `ipx isdn2 association show` and press <Enter>.

You see

```
                    IPX Association Table

Node Address Circuit Name  IPX      RIP   SAP  Warning
100000000000  admin        enabled  off   off     13
000000000001  personnel    enabled  off   off     13
```

To see more detailed information about a particular entry, including warnings, enter the node address immediately after the command, as follows:

```
ipx isdn2 association show 100000000000
```

When you press <Enter>, you see

```
Node         : 100000000000     Network     : 10000000
Circuit Name : admin            RIP         : off
IPX          : enabled          SAP         : off
```

IPX interface sub-context commands

circuit (ci)

Command purpose

The `ipx isdn2 circuit` command lets you use a circuit name to relate a circuit and a node or network address.

> ***Note:*** The circuit command and the `association table` are different ways of accessing the same information.

Command syntax

The syntax of the `circuit` command is as follows:

```
HomeOffice: ipx isdn2 circuit
```

Using the command

Changing circuit information

1 To change an entry in the IPX circuit table, enter `ipx isdn2 circuit` followed by the name of the circuit you want to change.

If you do not know the name of the circuit, enter * to display a list of valid entries.

The router prompts you for the node address.

```
Node <12 hex digits, name or *> :
```

2 Enter the node address for the circuit you want to change.

The router prompts for the following information:

```
IPX <ENABLED or DISABLED> (enabled) :
```

3 Define if you want IPX to be enabled on this interface.

The router prompts for the following information:

```
RIP mode <BROADCAST, TRIGGERED or
OFF> (triggered) :
```

IPX interface sub-context commands
circuit (ci) (continued)

4 Define which RIP mode you require on this circuit.

The router prompts for the following information:

```
SAP mode <BROADCAST, TRIGGERED or
OFF> (triggered) :
```

5 Define which SAP mode you require on this circuit.

Displaying the IPX circuit table

To display the IPX circuit table, enter `ipx isdn2 circuit show`.

The display looks like this:

```
IPX Association Table

Circuit Name  Node Address    IPX     RIP  SAP Warning

admin         100000000000    enabled  off  off    13
manufacturing <not assigned>  disabled  -    -      -
personnel     000000000001    enabled  off  off    13
```

To display a particular entry in more detail, including warnings, enter the circuit immediately after the command. For example:

```
ipx isdn2 circuit show admin
```

When you press <Enter>, you see

```
Circuit Name : admin         Network  : 10000000
Node         : 100000000000  RIP      : off
IPX          : enabled       SAP      : off
```

IPX interface sub-context commands

datalink (d)

Command purpose

The `ipx eth1 datalink` command lets you specify which IPX data link layer to use on your network.

Command syntax

The syntax of the `datalink` command is as follows:

```
HomeOffice: ipx eth1 datalink [show]
```

Using the command

Selecting the data link layer

1 To define which data link layer is used on your network, enter `ipx eth1 datalink.`

The router prompts as follows:

```
Datalink layer <ETHER2, 802.2, SNAP or
802.3> (802.3):
```

2 Select a data link layer to match the data link layer you have configured on your servers and workstations.

The following table lists the possible values:

Value	Description
`ETHER2`	IPX uses a unique packet header (type code). This value is suitable for networks that involve DEC or the TCP/IP protocol.
`802.2`	The router uses the IEEE and OSI standard 802.2 frame type. 802.2 is the default value.
`SNAP`	The router uses the IEEE and OSI standard 802.2 frame type with the 802.2 SNAP extension.
`802.3`	The router uses a standard Novell frame on a network that uses only NetWare.

IPX interface sub-context commands
datalink (d) (continued)

Displaying the current data link layer

To display the current data link layer, enter `ipx eth1 datalink show`.

The following appears:

```
Datalink layer : 802.3
```

IPX interface sub-context commands

diat (di)

Command purpose

The `ipx diat` command is available on the ISDN interface. It configures Dynamic IPX Address Translation (DIAT) for single-host or multi-host use on a specified circuit. It also enables and disables DIAT.

DIAT is enabled by default.

Command syntax

The syntax of the `diat` command is as follows:

```
HomeOffice: ipx isdn2 diat
```

Using the command

1 To configure IPX DIAT, enter `ipx isdn2 diat`.

The router prompts as follows:

```
Circuit name <up to 15 Characters or *> : default
```

2 Type the name of the circuit for which you want to change the DIAT parameters.

The router prompts as follows:

```
DIAT mode <DISABLED, SINGLEHOST or MULTIHOST>
(multihost) :singlehost
```

3 Do the following:

If	Then
only one computer is connected to the router	enter `singlehost`.
more than one computer is connected to the router	enter `multihost`.

When you have made your selection, the changed configuration appears:

```
Circuit updated:
Circuit Name : default
DIAT Mode : singlehost
```

IPX interface sub-context commands

enabled (e)

Command purpose

The `ipx <interface> enabled` command lets you enable and disable IPX routing on an interface.

This command is available on all interfaces and works identically on each of them.

Command syntax

The syntax of the `enabled` command is as follows:

```
HomeOffice: ipx eth1 enabled [show]

HomeOffice: ipx isdn2 enabled [show]
```

Using the command

Enabling or disabling IPX

1 To enable or disable IPX on an interface, enter `ipx <interface> enabled`, where <interface> is either `eth1` or `isdn2`.

The router prompts as follows:

```
Enable IPX on interface <YES or NO> (yes) :
```

2 Enter `yes` if you want IPX to be enabled on this interface, or `no` if you want it to be disabled.

The change does not take effect until you restart the router.

IPX interface sub-context commands
enabled (e) (continued)

Displaying IPX status on interfaces

To display a table showing the interfaces on which IPX is enabled, enter `ipx <interface> enabled show`, where <interface> is either `eth1` or `isdn2`.

The following appears:

```
IPX Protocol Table

Interface    Enabled     Current
eth1         yes         enabled
isdn2        yes         disabled
bridge       yes         disabled
```

IPX interface sub-context commands

lookup (l)

Command purpose

The `ipx isdn2 lookup` command displays the last 20 lookup failures recorded in the association table.

Command syntax

The syntax of the `lookup` command is as follows:

```
HomeOffice: ipx isdn2 lookup
```

Using the command

A lookup failure occurs when there is no association for a given remote network. Lookup failures may indicate an incorrect configuration or the failure of a WAN link. This information may be useful if you are having trouble communicating with a particular destination.

To display the lookup failures, enter `ipx isdn2 lookup`.

The display looks like this:

```
IPX Association Lookup Failures

Next hop router  Circuit  Fails   Last fail   Reason

274593854628       -        5     7d 0h    Circuit not defined
router.91        paris     10     1d 12h   IPX disabled on circuit
router.43        berlin     1     10m 1s   Circuit disabled
13460122034        -       25         2s   Circuit not defined
```

Parameters are described in the following table.

Parameter	Description
Fails	Tells you how many association lookups have failed for this circuit.
Last fail	Tells you how long ago the last failure occurred.

IPX interface sub-context commands

rip (ri)

Command purpose

The `ipx <interface> rip` command lets you configure the Routing Information Protocol (RIP). Normally, you will want to run RIP on the LAN interface(s). On the WAN interfaces, you may want to disable RIP to save costs.

This command is available on all interfaces.

Command syntax

The syntax of the `rip` command is as follows:

```
HomeOffice: ipx eth1 rip [show]

HomeOffice: ipx isdn2 rip [show]
```

Using the command

Enabling or disabling RIP

1 To enable or disable RIP, enter `ipx <interface> rip` where <interface> is either `eth1` or `isdn2`.

The router prompts as follows:

```
RIP <ON or OFF> (off) :
```

2 Enter `on` if you normally want RIP to run, or `off` if you do not want it to run at all.

The router prompts as follows:

```
Ignore incoming RIP updates <yes or no> (no) :
```

3 Respond as required.

The router prompts as follows:

```
Triggered Retry Count <5 - 100 or INFINITY> (5) :
```

Note: The triggered option is not available on Ethernet interfaces.

IPX interface sub-context commands
rip (ri) (continued)

4 Define the number of times that RIP tries to connect with RIP on the destination router if they cannot communicate (for example, due to failure in communications).

The router prompts as follows:

```
Triggered Retry Interval in minutes <1-10> (1) :
```

5 Define the time interval between triggered retry attempts.

The changes are confirmed as follows:

```
RIP updated:

   RIP                        : on
   Ignore incoming RIP updates: no ****************
   Triggered Retry Count      : 5
   Triggered Retry Interval   : 1 minutes
```

This change takes effect the next time the unit software is restarted using `top boot`.

Displaying RIP status

To display the status of RIP on all interfaces, enter `ipx <interface> rip show`.

A display similar to the following appears:

```
Routing Information Protocol
Interface  RIP  Retry Count  Retry Interval  Ignore Update
* eth1       on          -               -              -
=>  isdn2    on          5               1             No
sync2        off         5               1             No
bridge       on          -               -              -

Entries marked '*' will take effect the next time the unit
is restarted.
```

The arrow points to the current interface. The default is for RIP to be `OFF` on the WAN and running on the LAN.

IPX interface sub-context commands

sap (sa)

Command purpose

Service Advertising Protocol (SAP) provides devices on the network with information about available services and the devices that provide them. Normally, you will want to run SAP on the LAN interface(s). On the WAN interfaces you may want to disable SAP to save WAN costs.

The `ipx <interface> sap` command lets you specify how SAP operates over this interface. It is available in all contexts.

Command syntax

The syntax of the `sap` command is as follows:

```
HomeOffice: ipx eth1 sap [show]

HomeOffice: ipx isdn2 sap [show]
```

Using the command

Configuring SAP

1 To configure SAP on an interface, enter `ipx <interface> sap` where <interface> is either `eth1` or `isdn2`.

The router prompts as follows:

```
SAP <ON or OFF> (off) :
```

2 Enter `on` if you normally want SAP to work on this interface, or `off` to disable SAP.

The default is for SAP to be disabled on the WAN and enabled on the LAN.

IPX interface sub-context commands
sap (sa) (continued)

Note: The next two prompts appear only if you are modifying the isdn2 interface.

```
Triggered Retry Count <5 - 100 or INFINITY> (5) :
```

3 Define the number of times that SAP tries to connect with SAP on the destination router if they cannot communicate (for example, due to failure in communications).

The router prompts as follows:

```
Triggered Retry Interval in minutes <1-10> (1) :
```

4 Define the time interval between triggered retry attempts.

The router confirms the changes.

```
SAP updated:

   SAP                       : on
   Triggered Retry Count     : 5
   Triggered Retry Interval  : 1 minutes
```

This change takes effect the next time the unit software is restarted using `top boot`.

Displaying SAP status

To display the current state of SAP on all interfaces, enter `ipx <interface> sap show` where <interface> is either `eth1` or `isdn2`.

When you press <Enter>, you see a screen similar to the following:

```
Service Advertising Protocol

    Interface      SAP         Retry      Retry
                               Count      Interval
    eth1           on          -               -
=>  isdn2          off         5               1
    bridge         off         5               1
```

Network context shell commands

The `network context` manages the router's physical interfaces. The commands are grouped into sub-contexts, one for each interface. The sub-contexts depend on the number and type of interfaces installed on your router. Network sub-contexts are:

Sub-context	Description
general	Configure use of WAN links on the router.
eth1	Manage an Ethernet interface.
isdn2	Manage an ISDN interface.

Some protocols need to have certain parameters set up separately for each interface. Commands dealing with these parameters are not described in the `network context` but in the protocol-specific contexts.

Network general sub-context commands

The `network general` sub-context lets you manage the Point-to-Point Protocol.

In the `network general` sub-context, the command prompt is:

```
HomeOffice: network general
```

The following commands are described in this section:

Command	Shortcut	Description
decode	d	Collects specified types of packets in the system trace buffer and decodes them for analysis.
multilink	m	Configures PPP Multilink box-wide.
ppp	pp	Configures PPP box-wide.

To display a list of available commands, enter `help`. To return back to non-privileged level, enter `quit`.

Network general sub-context commands

decode (d)

Command purpose

The `network general decode` command collects and decodes a variety of information packets. This command will most likely be used by experienced network administrators or technical support personnel for diagnostic purposes.

> ***Note:*** If you enable this feature, it significantly reduces the performance of your router.

Command syntax

The syntax of the `decode` command is as follows:

```
HomeOffice: network general decode
```

Using the command

1 To initiate packet collection, enter `network general decode`.

The router prompts for the type of packets to be collected.

```
Type of decode <Combine l, p, d, b, f, o, m, c, a,
 L, P, D, B, F, O, M, C, A or 'off'> (off) :
```

The parameters are described in the following table.

Parameter	Description
a	Enables tracing at all levels.
b	Collects BAP and BACP packets in the system trace buffer.
c	Traces packets above the compression level.
d	Collects data packets in the system trace buffer.
f	Collects the first packet sent when the link opens (that is, the one that opens the call).
l	Collects LCP negotiation packets in the system trace buffer.

—continued—

Network general sub-context commands
decode (d) (continued)

Parameter	Description
m	Traces packets above the multilink level.
o	Collects packets at the outermost level (below multilink, compression, and so on). This is the default level.
p	Collects Echo Requests and LQM packets in the system trace buffer.
A	Enables tracing and decoding at all levels.
B	Collects BAP and BACP packets in the system trace buffer and decodes them.
C	Traces packets above the compression level and decodes them.
D	Collects data packets and decodes them.
F	Collects and decodes the first packet sent when the link opens.
L	Collects LCP negotiation packets and decodes them.
M	Traces packets above the multilink level and decodes them.
O	Collects packets at the outermost level (below multilink, compression, and so on) and decodes them.
P	Collects Echo Requests and LQM packets, and decodes them.
—end—	

2 Enter the type of packet(s) you want to collect, or enter `off` if you want to disable the decode function.

The router prompts you for the circuits from which to collect packets.

```
Circuit's context or ALL circuits (ALL) :
```

You can choose to collect packets from a particular circuit or from all circuits.

Network general sub-context commands
decode (d) (continued)

3 Enter the context from which you want to select a circuit or select all circuits.

You see a display confirming which type of packet you are collecting, for example:

```
PPP decode : D
```

If you choose a particular context (for example, the `isdn2` *context), the router prompts you for the name of the circuit in that context from which you want to collect packets.*

4 Enter the name of the circuit. For example

```
Circuit name (NONE) : nortel1
```

You see a display confirming which type of packet you are collecting, the name of the circuit, and the context you have chosen.

```
PPP decode : D
Circuit    : nortel1 (isdn2)
```

Displaying decode status

To determine if the decode function is enabled or not, enter `network general decode show`.

For example, if the decode function is not enabled, you see

```
PPP decode : off
```

Network general sub-context commands

multilink (m)

Command purpose

The `network general multilink` command lets you set up the PPP Multilink feature on your router. You can use multilink to

- combine links into a multilink bundle
- sequence packets

Note 1: Before configuring PPP Multilink on your router, make sure you have configured two virtual circuits. These can either be two ISDN virtual circuits or an ISDN link aggregated with a leased line.

Note 2: In order for PPP Multilink to work, PPP Multilink negotiation must be enabled at both ends of the link.

Command syntax

The syntax of the `multilink` command is as follows:

```
HomeOffice: network general multilink
```

Using the command

Enabling PPP multilink

1 To enable PPP multilink, enter `network general multilink`.

The router prompts as follows:

```
Negotiate PPP Multilink option <enabled or
disabled> (disabled):
```

2 Type `enabled` to set up PPP Multilink negotiation on your router.

If negotiation is successful, PPP Multilink combines all available channels into a multilink bundle.

The router prompts as follows:

```
Negotiate discriminator option <enabled or
disabled> (enabled):
```

3 Enter `ENABLED`.

When the discriminator option is enabled, each end of each link identifies itself, to help bundle together links.

Network general sub-context commands
multilink (m) (continued)

The router prompts as follows:

```
Negotiate short sequence number option <enabled or
disabled> (disabled):
```

Usually packets are transmitted with 24-bit sequence numbers when they are negotiated through PPP. If you have configured both units for short sequence numbers by selecting ENABLED at both ends of the link, a 12-bit sequence number will be negotiated. This makes the frame smaller so that there is less data to transmit.

If you are combining links that have different transmit times, for example, a transatlantic leased line augmented with a satellite ISDN link, you should disable this option. This is because packets are sent at different speeds along these lines and a short sequence number would cause the packets to lose their synchronization.

4 Enable or disable the short sequence number option as required.

The router prompts as follows:

```
Negotiate Bandwidth Allocation Protocol <ENABLED or
DISABLED> :
```

5 Enable or disable the Bandwidth Allocation Protocol on your router as required.

To fine tune individual circuits, use the bap command. You have now configured PPP Multilink to work on your router.

Fine tuning PPP multilink

To carry out fine-tuning of PPP Multilink, change to the `network isdn2` sub-context and use the `multilink` command. This lets you configure functions such as packet fragmentation, packet ordering, and omission of compression for a single link.

You can carry out further fine-tuning by using the `ppp` command in the `network general` sub-context. Use this command to configure address and control field compression, and protocol field compression.

Note: Users performing fine-tuning of PPP Multilink should have greater networking experience than those just configuring PPP Multilink to work on their unit.

Network general sub-context commands

ppp (pp)

Command purpose

The `network general ppp` command is available in the `network general` and `network <interface>` sub-contexts. It is an abbreviation of Point-to-Point Protocol.

Use `network general ppp` to

- enable Address and Control Field Compression
- enable Protocol Field Compression

Note: If you have configured PPP Multilink to run on your unit using the `network general multilink` command, you can use `network general ppp` to carry out further fine-tuning on your multilink packets. Refer also to the `multilink` command in the `network isdn2` context.

Command syntax

The syntax of the `ppp` command is as follows:

```
HomeOffice: network general ppp
```

Using the command

1 To set up compression, enter `network general ppp`.

The router prompts as follows:

```
Address and Control Field Compression <ENABLED or
DISABLED> (disabled):
```

2 Enable this option to compress the address and control field of a frame.

This also applies to multilink frames.

The router prompts as follows:

```
Protocol Field Compression <ENABLED or
DISABLED> (disabled):
```

The default is `DISABLED`.

Network general sub-context commands
ppp (pp) (continued)

3 Enable this option to compress the protocol field of a frame.

If you are running PPP Multilink, the multilink headers in your multilink frames are compressed, along with any other protocol headers in the frame.

Note: Enabling Address and Control Field Compression and Protocol Field Compression may cause interoperability problems with other vendors' equipment. If you experience problems, you may choose to disable them.

The router prompts as follows:

```
Authentication Restart Timer in seconds <1 - 255>
(10) :
```

4 Respond as required.

Network interface sub-context commands

The commands in the `network <interface>` sub-context let you manage the router's interface(s).

In the `network <interface>` sub-context, the command prompts are:

```
HomeOffice: network eth1
```

```
HomeOffice: network isdn2
```

The following commands are described:

Command	Shortcut	Interface type	Description
activate	ac	isdn2	Initiates dialing from a HomeOffice Router to a peer device.
address	ad	eth1 isdn2	Displays or configures the physical address for an interface.
alias	al	eth1 isdn2	Changes the name of this sub-context.
bap	ba	isdn2	Fine tunes the Bandwidth Allocation Protocol (BAP).
callback	cb	isdn2	Configures the callback feature.
calls	ca	isdn2	Displays information about calls made on ISDN.
circuit	ci	isdn2	Creates a circuit to a remote destination. With this command, you can create PBX, voice, or data circuits.
configure	conf	eth1 isdn2	Configures the router to match the WAN service used.
default	d	isdn2	Sets default call idle and non-preemption timers.

—continued—

Command	Shortcut	Interface type	Description
enabled	e	eth1 isdn2	Enables or disables an interface.
multilink	m	isdn2	Configures multilink parameters on a circuit.
ppp	pp	isdn2	Configures the PPP protocol.
rates	rat	isdn2	Monitors calls made and received by the router dynamically.
rejects	rej	isdn2	Displays information about incoming and outgoing calls.
security	sec	isdn2	Uses PAP or CHAP network security.
statistics	ss	eth1	Displays octet and packet values for the Ethernet interface.
status	st	eth1 isdn2	Displays information about the ISDN or Ethernet connection.
test	te	isdn2	Tests ISDN circuits.
timer	ti	isdn2	Configures the waiting time of the backup and failed circuit retry timer.
tune	tu	isdn2	Fine tunes the parameters used by a circuit.
vcs	v	isdn2	Displays information about virtual circuits.
—end—			

To display a list of available commands, enter `help`. To exit back to non-privileged level, enter `quit`.

Network interface sub-context commands

activate (ac)

Command purpose

The `network isdn2 activate` command initiates dialing from a HomeOffice Router to a Rapport Dialup Switch 112. It is possible for a link to be enabled, but not active. If this is the case, the router at one end of the link will not make or receive calls, but spoofing packets will continue to be sent across the link. The `network isdn2 activate` command allows the user to control when the security dialog boxes are presented by Local Manager.

It is essential that you activate the link if you are using a SecurID/Digital Pathways server for security authentication. If you do not, the router will be unable to dial the dialup switch, and a call will not be made.

Command syntax

The syntax of the `activate` command is as follows:

```
HomeOffice: network isdn2 activate
```

Using the command

1 To initiate a call, enter `network isdn2 activate.`

The router prompts as follows:

```
Circuit name <up to 15 Characters or *> :
```

2 Enter name of the circuit you want to use.

The router prompts as follows:

```
Activate circuit <YES or NO> (yes) :
```

3 Enter `yes` or `no` as required.

The active state is shown:

```
Active state updated:
    Active interface: no
```

Network interface sub-context commands

address (ad)

Command purpose

The `network <interface> address` command displays the physical address of Ethernet and ISDN interfaces. For ISDN interfaces, this command can be used to change the ISDN address of an interface.

The command works differently, depending in which sub-context it is used.

Command syntax

The syntax of the `address` command is as follows:

```
HomeOffice: network eth1 address [show]

HomeOffice: network isdn2 address [show]
```

Using the command

Displaying the Ethernet interface

To display the Ethernet address and state of the Ethernet interface, enter `network eth1 address`.

The following appears:

```
Ethernet address : 0800390241C2
Interface state  : enabled
```

The router's Ethernet address is its physical address on the Ethernet LAN. Since it is allocated by the router, you cannot change it.

Changing the ISDN interface

In an ISDN network, the `network isdn2 address` command records the ISDN address allocated by your ISDN service provider and changes the router's ISDN address. You can also use this command to allocate a sub-address.

Note: An ISDN address must be assigned for the interface to be enabled.

1 To change the ISDN address, enter `network isdn2 address`.

If you are running	Then
National ISDN-1 or 5ESS Custom Multipoint (see the `system isdn` command)	you will be asked to enter the ISDN address and SPID (Service Profile Identifier) for each B-channel. ***Note:*** For National ISDN-1, you can also use the auto-detect feature to determine the address and SPID.
National ISDN-2	you will be asked to enter a single ISDN address and SPID.

```
Address information for channel 1
Interface ISDN address <up to 41 digits> (5551234) :
```

The address and SPID should have been assigned by your ISDN authority. If you use sub-addressing, add the sub-address to the end of the address, separated by a hyphen. An example of an ISDN address with a sub-address is: 0315551234-1.

Note: If you decide that you want to turn ISDN sub-addressing off later, use the `network isdn2 address` command. Re-type the ISDN address without the sub-address.

2 Enter the ISDN address for channel 1.

```
SPID for this address <up to 20 digits, NULL or
Auto> (555123411) :
```

Network interface sub-context commands
address (ad) (continued)

3 Enter the SPID for channel 1, or if you are using National ISDN-1, enter `auto`.

For National ISDN-1, the router prompts you for a second ISDN address and SPID.

```
Address information for channel 2
Interface ISDN address <up to 41 digits> (5552345) :
```

4 Enter the ISDN address for channel 2.

```
SPID for this address <up to 20 digits, NULL or
Auto> (555234511) :
```

5 Enter the SPID for channel 2, or if you are using National ISDN-1, enter `auto`.

The router prompts as follows:

```
Maximum transmission unit <576 or 1500> (576) :
```

6 Enter an appropriate MTU for your network.

Possible values are `576` and `1500`. On an ISDN interface, you should select `1500`, unless you have to use poor quality lines with a lot of errors on the link. In this case, select `576` for optimum throughput.

Displaying the ISDN address configuration

To display the current ISDN address configuration on an interface, enter `network isdn2 address show`.

A display similar to the following appears:

```
ISDN address configuration details:
  Interface ISDN address    : 246102121162
  Interface MTU size        : 576
  Interface state           : enabled

Integrator: network isdn2
```

Network interface sub-context commands
address (ad) (continued)

If you are running National ISDN-1 or 5ESS Custom Multipoint, the router displays your current ISDN address configuration on each interface. (If you are running National ISDN-2, you will only have a single ISDN address and SPID.) You see

```
ISDN address configuration:
    Interface ISDN address 1    : 5549424
    Interface ISDN SPID 1       : 12345
    Interface ISDN address 2    : 1031
    Interface ISDN SPID 2       : 103122
    Interface MTU size          : 1500
    Interface state             : enabled
```

Network interface sub-context commands

alias (al)

Command purpose

The `network <interface> alias` command allows you to change the name of the interface sub-context. You may want the sub-context name to reflect the part of the network to which this context gives access, or you may want to use a name that is more appropriate in your own language. Changing the name of this context also changes the name of any other context with the same name. For example, you may want to change the name of `network eth1` to `local`.

> ***Note:*** You can still use the original name of the sub-context. The sub-context can have more than one name.

This command is available in all `network` sub-contexts and operates identically in each.

Command syntax

The syntax of the `alias` command is as follows:

```
HomeOffice: network eth1 alias

HomeOffice: network isdn2 alias
```

Using the command

1 To rename the interface sub-context, enter `network <interface> alias` where <interface> is either `eth1` or `isdn2`.

The router prompts as follows:

```
Rename eth1 context <up to 7 characters> (eth1):
```

The name you choose can have a maximum of seven characters. The router rejects any name that clashes with the name or short form of a command or other context.

Network interface sub-context commands
alias (al) (continued)

2 Enter the new name.

The new name appears.

If you enter `local` and press <Enter>, you see

```
eth1 context updated.
network local
```

If you do this, all of the `<protocol> eth1` sub-contexts are also renamed `local`.

Network interface sub-context commands

bap (ba)

Command purpose

The `network isdn2 bap` command fine tunes the Bandwidth Allocation Protocol (BAP) on your router. This protocol is used when extra bandwidth is needed to cope with data flow (for example, with bandwidth aggregation). It ensures that both ends of a link agree on when to open or close additional links.

Command syntax

The syntax of the `bap` command is as follows:

```
HomeOffice: network isdn2 bap
```

Using the command

1 To configure BAP, enter `network isdn2 bap`.

The router responds as follows:

```
Circuit name <up to 15 Characters or *> :
```

2 Enter the name of the circuit you want to configure.

The router responds as follows:

```
Use default circuit's configuration <YES or
NO> (yes):
```

3 Enter `yes` if you have set up a default circuit and want to use its configuration.

The router responds as follows:

```
Retry timer in seconds <1 - 10> (2) :
```

4 Enter the number of seconds that should elapse between retransmissions.

You may need to retransmit the packet if there is no response from previous attempts.

The router responds as follows:

```
Maximum number of Requests or Indications
sent <1 - 3> (2) :
```

Network interface sub-context commands
bap (ba) (continued)

5 Enter the number of BAP requests or indications that should be sent if there is no response to previous attempts.

The default value is 2.

The router responds as follows:

```
Status timer in seconds <1 - 120> (20) :
```

6 Enter the number of seconds the router should wait for a call status indication after you have agreed to receive the call.

The router responds as follows:

```
Don't ask peer for phone number <ENABLED or
DISABLED> (disabled) :
```

7 Disable this option if you specifically do not want the peer to suggest a phone number; otherwise, select `enabled`.

The configuration of the circuit appears. For example:

```
Circuit updated:

Circuit name                          : bap1
   Use default circuit's configuration : no
   Retry timer in seconds             : 3
   Maximum Requests to be sent        : 2
   Status timer in seconds            : 34
   Don't ask peer for phone number     : enabled
```

Network interface sub-context commands

callback (cb)

Command purpose

The `network isdn2 callback` command provides a mechanism to disable callback on all the circuits on a particular ISDN interface. It is enabled by default.

You must use this command to enable any callback configuration that has been made using the `circuit` command.

Command syntax

The syntax of the `callback` command is as follows:

```
HomeOffice: network isdn2 callback
```

Using the command

1 To enable or disable callback, enter `network isdn2 callback`.

The router responds as follows:

```
Allow outgoing callback requests <DISABLED or
ENABLED> (enabled) :
```

2 Enable outgoing callback requests that you have configured with the `circuit` command.

The router responds as follows:

```
Accept incoming callback requests <DISABLED or
ENABLED> (enabled) :
```

3 Enable incoming callback requests that you have configured with the `circuit` command.

You see an updated display of the command.

```
Interface callback parameters updated.

Allow outgoing callback requests  : enabled
   Accept incoming callback requests : disabled
```

Network interface sub-context commands

calls (ca)

Command purpose

The `network isdn2 calls` command is available on ISDN interfaces. It displays the same information about the calls made across these interfaces to remote destinations.

Command syntax

The syntax of the `calls` command is as follows:

```
HomeOffice: network isdn2 calls [<destination circuit name>]
```

Using the command

network isdn2 calls

The displays are similar for all interfaces:

```
WAN Call Statistics

Remote            Successful  Successful Total     Current
router            Calls out   Calls in   duration  duration
L Listener                0           0          -         -
P Manufacturing          36          33  23h 1m 34s      54s
```

Note: The listener circuit is marked with `L`. The listener answers all incoming ISDN calls. It performs the basic authorization that identifies the calling party. The last two values displayed are described in the following table.

Call value	Description
Total duration	This is the total time of calls between this router and the remote router.
Current duration	This is the length of time the current call has been in existence.

Network interface sub-context commands
calls (ca) (continued)

network isdn2 calls <destination circuit name>

To display more information about calls to a particular destination, enter `call` followed by the destination circuit name. For example:

```
Call      Calls          Call           Calls          Calls
          accepted       duration       rejected       now
Out             21             -      0 [ 0.00%]         0
In              17             -      0 [ 0.00%]         0

All calls  Transmitted   rate/s       Received   rate/s

Packets              0         -              0         -
  Bridge     0 [ 0.00%]         -     0 [ 0.00%]         0
  IP         0 [ 0.00%]         -     0 [ 0.00%]         0
  IPX        0 [ 0.00%]         -     0 [ 0.00%]         0
Octets
  Bridge     0 [ 0.00%]         -     0 [ 0.00%]         0
  IP         0 [ 0.00%]         -     0 [ 0.00%]         0
  IPX        0 [ 0.00%]         -     0 [ 0.00%]         0
```

Note: The statistics displayed do not include calls made or received using the `isdn2 test` command.

Network interface sub-context commands

circuit (ci)

Command purpose

The `network isdn2 circuit` command is used to configure the Circuit table for each interface. The Circuit table contains the information the router needs to make connections with remote destinations. In particular, it lets you associate the physical address (ISDN) of a remote destination with a name.

Three types of circuits may be created:

- voice circuits
  Voice circuits are used with analog devices such as telephones or fax machines.
- data circuits
  Data circuits are used with digital devices such as the HomeOffice Router.
- PBX circuit
  The PBX circuit is used with the Meridian digital telephone. Only one PBX circuit can be configured.

Command syntax

The syntax of the `circuit` command is as follows:

```
HomeOffice: network isdn2 circuit <action>
```

where `<action>` is either `add`, `change`, `delete`, `change`, or `show`.

Using the command

Adding a voice or data circuit

1 To add a voice or data circuit to the circuit table, enter

```
network isdn2 circuit add
```

The router responds as follows:

```
Circuit Name <Up to 15 Characters or *> :
```

Network interface sub-context commands
circuit (ci) (continued)

2 Enter a name for the circuit.

Each circuit must have a name. Use this name to refer to the circuit when setting up protocol-specific information in the `protocol interface` sub-contexts.

The router responds as follows:

```
Circuit type <DATA, VOICE or PBX> (data) :
```

3 Select `voice` or `data`.

Choose `voice` to configure this circuit for use with a telephone. Choose `data` to configure the circuit for a digital device.

The ISDN service distinguishes between these configurations.

The router responds as follows:

```
Outgoing call type <64KBPS, 56KBPS, SPEECH,
3.1KAUDIO> (64kbps):
```

4 Respond as required.

The router responds as follows:

```
ISDN address to call <Up to 41 digits or DISABLED> :
```

5 Enter the address the router should use when making a call to the remote destination.

Ensure that you include any necessary codes.

The router responds as follows:

```
ISDN address received <Up to 41 digits or NULL> :
```

As a security measure, the network can use Calling Line Identification (CLI) to identify the calling unit to the called unit.

Note: Caller ID is the North American equivalent of CLI.

When an ISDN device receives a call, it checks the address of the calling unit to see if it recognizes it. If it does not, it does not take the call.

6 Enter the address the router should expect in calls from the unit at the other side of this circuit.

Ensure that you include any necessary area codes.

Network interface sub-context commands
circuit (ci) (continued)

The remote sub-address should be included only if the switch forwards the calling sub-address.

Note: If you include the remote sub-address in the `ISDN address received`, and the switch does not forward the calling sub-address, then the circuit will fail to come up and will be logged as an incoming reject under `Authentication refused`.

The router responds as follows:

```
Use multiple ISDN addresses <NO or YES> (no) :
```

7 Enter `yes` only if you are using National ISDN-1 (Basic Rate) and if you have two ISDN addresses (one for each B-channel).

The router prompts you for the address to call and the address received (as above).

If you are not sure what to enter here, try making a call from the remote unit to this one. The router rejects the call and notes that it has done so in its Rejects table. Use the `rejects` command to find out the address of the router that made the rejected call, and enter it here.

The router responds as follows:

```
Circuit state <DISABLED or ENABLED> (enabled)
```

8 Respond as required.

```
Default active state <INACTIVE or ACTIVE> active) :
```

9 Respond as required to define the default state of the circuit.

The default state is resumed if the HomeOffice Router is rebooted and the interim configuration is lost. The default state should be disabled when using third-party security authentication so that you can control when to disable or enable the circuit and the authentication process.

The router responds as follows:

```
Circuit type <PRIMARY or SECONDARY> (primary) :
```

10 Respond as required.

The router responds as follows:

```
Use default circuit's configuration <YES or
NO> (yes):
```

Network interface sub-context commands
circuit (ci) (continued)

11 Press <Enter> if you want your circuit to use the configuration of the default circuit.

No further prompts appear if you choose to adopt the default circuit's configuration; otherwise, the router responds as follows:

```
Compression <DISABLED, NEGOTIATE, SPIDER or STAC>
(negotiate) :
```

12 Choose the compression method.

Data compression allows you to send data more efficiently between two devices.

If	Then
you choose `negotiate`	the router negotiates a compression algorithm with the remote unit.
you would prefer to specify the compression algorithm to be used	choose either `PREDICTOR`, `SPIDER`, or `STAC`, depending on what type of compression the other unit is running.
you choose anything other than `disabled`	two more compression-related prompts appear.

```
Compression with multilink <BUNDLE or
LINK> (bundle) :
```

13 Choose the compression with multilink method.

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

Network interface sub-context commands
circuit (ci) (continued)

Compression method	Description
`link` (compression after Multilink)	This means that data is compressed separately at each link. Choose `LINK` if the remote device's circuit is running over a Primary Rate ISDN card that performs hardware compression (such as a Rapport Dialup Switch 112). By choosing `LINK` you can take advantage of the faster compression in the remote Primary Rate ISDN card. This can result in improved overall throughput, despite the slightly less effective compression.
`bundle` (sometimes called compression before Multilink)	This means that data is compressed before the packets are split onto the different links of the call. Bundle compression provides the better compression ratio. You should choose `BUNDLE` if your router is interoperating with • a Rapport Dialup Switch 8E • a Rapport Dialup Switch 112 (using software compression) • another router

```
Notify compression error <RESET-REQUEST or
CONFIG-REQUEST> (reset-request) :
```

14 Choose the default `reset-request` unless you know that the remote unit uses `config-request` to notify the occurrence of a compression error.

The router responds as follows:

```
Bridging on circuit <DISABLED or
ENABLED> (enabled) :
```

Network interface sub-context commands
circuit (ci) (continued)

15 Press <Enter> if you wish to bridge over this interface.

The router responds as follows:

```
Routing on circuit <DISABLED or
ENABLED> (disabled) :
```

16 Type `enabled` if you wish to route over this circuit.

The router responds as follows:

```
Support for triggered RIP and SAP <DISABLED or
ENABLED> (disabled) :
```

Triggered RIP and SAP are methods of keeping costs down on ISDN WANs. Normally, RIP and SAP are used on a network to pass on messages to other units. Every 30 seconds or every minute, a message sent to these routers tells them that the source router is active and viable. Although this is useful on leased lines, it is expensive on ISDN circuits where charges are made according to transmission time.

Note: Triggered RIP and SAP must be enabled where the Multiple Static Routes feature is being used.

Instead of confirming availability at frequent intervals, routing information can be configured statically, in a routing table. This is an adequate solution for less complex networks. For more complex networks, where the configuration may change, triggered RIP and SAP management is used.

This is how it functions:

- On power-up, your HomeOffice Router and others exchange RIP information.
- Instead of repeating this information, they do not exchange packets until the configuration changes. Hence, configuration changes trigger an update.

Note: If the ISDN address to call is set to `DISABLED`, support for triggered RIP and SAP must be disabled as outgoing calls cannot be made on this circuit.

Network interface sub-context commands
circuit (ci) (continued)

17 Enable or disable triggered RIP and SAP as required.

The router responds as follows:

```
Callback <DISABLED, ACCEPT or REQUEST> (disabled) :
```

This prompt allows you to configure Callback on ISDN circuits. The example below shows ISDN default values. This is a cost-saving feature allowing you to take advantage of lower tariffs (where there is a discrepancy in the tariffs charged by the source and destination telephone companies).

18 Enter ACCEPT if you want to accept Callback at the local site, or REQUEST if you want to request that calls be returned from the remote site.

The router responds as follows:

```
Callback identification <CLI or PPP> (ppp) :
```

It is generally cheaper to operate Callback with CLI than with PPP. This is because CLI rejects the initial call and immediately dials back to the originating site; there is no charge made for this initiating call by most European PTTs. PPP accepts the initial call and negotiates callback with the originating site. However, PPP interoperates with other products; CLI may not.

Note: PPP must be running for Callback to work, regardless of whether you choose CLI or PPP at this prompt. If you choose PPP at this prompt, you must configure either PAP or CHAP for Callback to work.

Network interface sub-context commands
circuit (ci) (continued)

19 Select `CLI` or `PPP` as required.

The router responds as follows, depending on your response in step 18.

If you choose to	Then
accept Callback at the local site	*the router responds as follows:* `Delay before returning call in seconds <1 - 60> (1) :` Enter the length of time that you want to allow for incoming calls to be cleared.
request Callback from the remote site	*the router responds as follows:* `Maximum wait for returned call in seconds <5 - 120> (20) :` Enter the maximum length of time that you want to wait for the initial call to be returned. The data is queued until the remote unit returns the call or this period elapses.

The router displays details of the circuit you added.

```
Circuit added:
    Circuit name                : TMtest
    ISDN address to call        : 555 1212
    ISDN address received       : 555 3661
    Circuit state               : enabled
    Default active state        : active
    Circuit type                : primary
    Outgoing Call Type          : 64kbps

    Use circuit defaults        : yes
    Encapsulation               : ppp
    Compression                 : disabled
    Compression with multiline  : n/a
    Notify compression error    : n/a
    Bridging                    : disabled
    Routing                     : enabled
    Support for RIP and SAP     : disabled
    Callback                    : accept
```

Network interface sub-context commands
circuit (ci) (continued)

```
Callback identification      : ppp
Delay before returning call  : 20

Use multilink defaults       : yes
Use PPP defaults             : yes

Use security defaults        : no
Use timer defaults           : yes
Use tune defaults            : yes
```

This example shows an ISDN circuit. The Tuning Parameters and the Bandwidth-on-demand criteria can be defined for all circuits on a router using the `default` command, and are set for individual circuits using the `tune` command.

Changing the pbx circuit

1 To make changes to the PBX circuit, enter

`network isdn2 circuit change`

The router responds as follows:

`Circuit name <up to 15 characters or *> (Meridian) :`

2 Enter `Meridian`.

The router responds as follows:

`Outgoing call type <64 KBPS or 56 KBPS> (56 Kbps) :`

3 Enter the speed at which outgoing calls should be made.

The router responds as follows:

`Your telephone number <up to 41 digits or NULL> :`

4 Enter the new telephone number, if required.

The router responds as follows:

`PBX telephone number <up to 41 digits or DISABLED> :`

5 Enter the ISDN address (phone number) that you need to dial to reach the PBX.

The router responds as follows:

`Accept calls from <up to 41 digits or DISABLED> :`

Network interface sub-context commands
circuit (ci) (continued)

6 Enter the ISDN address (phone number) of the PBX.

The router responds as follows:

```
Circuit state <DISABLED or ENABLED> (enabled) :
```

7 Define whether the circuit you are setting up is to be enabled immediately.

The default is `enabled`

The router displays the new configuration details.

Changing a voice or data circuit

Note: Most of the prompts in this procedure are the same as for `network isdn2 circuit add`. For more detailed information about what to enter at these prompts, see “Adding a voice or data circuit” on page 7-24.

To keep the values in subsequent prompts unchanged, press <Enter>.

1 To make changes to an existing circuit, enter

```
network isdn2 circuit change
```

The router responds as follows:

```
Circuit name <up to 15 characters or *> (isdn2) :
```

2 Enter the name that identifies the circuit you want to change.

The router responds as follows:

```
Outgoing call type <64K, 56K, SPEECH, 3.1K Audio> :
```

3 Respond as required.

The router responds as follows:

```
ISDN address to call <up to 41 digits or DISABLED> :
```

4 Enter the ISDN address (phone number) that you need to dial to reach the remote unit.

The router responds as follows:

```
ISDN address received <up to 41 digits or
DISABLED> :
```

Network interface sub-context commands
circuit (ci) (continued)

5 Enter the ISDN address (phone number) of the remote unit.

The router responds as follows:

```
Use multiple ISDN addresses <NO or YES> (no):
```

6 Enter `yes` if you are dialing to a National ISDN-1 connection and want to set up more than one ISDN address.

Note: This feature is only available in North America.

The router responds as follows:

```
Circuit state <DISABLED or ENABLED> (enabled) :
```

7 Define whether the circuit you are setting up is to be enabled immediately.

The default is `enabled`.

The router responds as follows:

```
Default active state <INACTIVE or ACTIVE> (active):
```

Each circuit on a router has a default active state. This is the state that will be resumed if the router is rebooted and interim configuration values are lost.

8 If you are using a security server, you should set the default active state to `inactive`.

Each circuit can then be activated individually.

The router responds as follows:

```
Circuit type <PRIMARY or SECONDARY> (primary) :
```

9 Respond as required.

The router responds as follows:

```
Use default circuit's configuration
<YES or NO> (yes) :
```

10 Press <Enter> if you want your circuit to use the configuration of the default circuit.

Network interface sub-context commands
circuit (ci) (continued)

No further prompts appear if you choose to adopt the default circuit's configuration.

If you choose no, the following compression prompts appear:

```
Compression <DISABLED, NEGOTIATE, PREDICTOR, SPIDER
or STAC> (negotiate):
```

```
Compression with multilink <BUNDLE or
LINK> (bundle) :
```

See "Adding a voice or data circuit" on page 7-24 for information about how to respond to these prompts.

The router responds as follows:

```
Notify compression error <RESET-REQUEST or
CONFIG-REQUEST> (reset-request) :
```

11 Choose the default `reset-request` unless you know that the remote unit uses `config-request` to notify the occurrence of a compression error.

The router responds as follows:

```
Bridging on circuit <DISABLED or
ENABLED> (enabled) :
```

12 Press <Enter> if you wish to bridge over this interface.

The router responds as follows:

```
Routing on circuit <DISABLED or
ENABLED> (disabled) :
```

13 Type `enabled` if you wish to route over this interface.

The router responds as follows:

```
Support for triggered RIP and SAP <DISABLED or
ENABLED> (disabled) :
```

14 Type `enabled` if you expect to run triggered RIP or triggered SAP.

We recommend that you use triggered mode. See "Adding a voice or data circuit" on page 7-24 for more information.

The router responds as follows:

```
Callback <DISABLED, ACCEPT or REQUEST> (disabled) :
```

This prompt enables you to configure Callback for the secondary circuit. See "Adding a voice or data circuit" on page 7-24 for more information.

Deleting a circuit

Note: You cannot delete default circuits.

1 To delete an entry from the circuit table, enter

```
network isdn2 circuit delete
```

The router prompts you to enter the name of the circuit.

2 Enter the name of the circuit you want to delete.

The router displays details of the circuit you have asked to delete, and waits for confirmation before deleting it.

```
Delete Circuit <YES or NO> :
```

3 Enter `yes`.

Changing the default circuit

To make changes to the default circuit, enter `network isdn2 circuit change default`.

Displaying circuit details

To display the circuit table for this interface, enter

```
network isdn2 circuit show
```

This displays the circuit table for this interface which looks like this:

```
                ISDN Circuit Table
Name        ISDN address to call    State     Type      Compress    Warn
Dallas      19721234567             enabled   primary   negotiate   -
Meridian    19057654321             enabled   pbx       disabled    -
admin       555                     enabled   primary   negotiate   -
default     n/a                     n/a       default   disabled    -
listener    n/a                     enabled   listener  disabled    -
voice       disabled                enabled   voice     disabled    -
```

The display above applies to an ISDN interface. This status also appears in the `calls` and `vcs` commands, and in the individual circuit display, as seen in the following note.

Network interface sub-context commands
circuit (ci) (continued)

Note: The listener circuit is used to receive calls when Calling Line Identification is not available. On an ISDN link, it accepts all incoming calls without CLI, or those with CLI that do not match any ISDN Address Received. It then checks the incoming call using PAP or CHAP. If you want to prevent the latter from being accepted and carrying out PAP or CHAP negotiations, you should disable the listener circuit.

Displaying the details for a specific circuit

To display an individual circuit, enter `network isdn2 circuit show` followed by the name of the circuit.

Full details of the circuit appear.

Network interface sub-context commands

configure (conf)

Command purpose

The `network <interface> configure` command lets you set up the physical parameters on the LAN and configure the router to match the WAN service to which you are attaching it.

This command is available on Ethernet and ISDN interfaces, and works differently in each.

Command syntax

The syntax of the `configure` command is as follows:

```
HomeOffice: network eth1 configure [show]

HomeOffice: network isdn2 configure [show]
```

Using the command

Configuring the Ethernet interface

This procedure allows you to enable bridging and/or routing on the router.

1 To define the router's physical parameters on the LAN, enter `network eth1 configure`.

The router prompts as follows:

```
Bridging on interface <ENABLED or
DISABLED> (enabled):
```

2 Type `enabled` if you want to enable bridging or `disabled` if you do not.

The router prompts as follows:

```
Routing on interface <ENABLED or
DISABLED> (disabled):
```

Network interface sub-context commands
configure (conf) (continued)

3 Type `enabled` if you want to enable routing or `disabled` if you do not.

When you have finished, the router displays the updated configuration.

```
Interface configuration updated:

Bridging on interface    : yes
   Routing on interface  : no
   Media type            : automatic
```

These changes do not take place until you restart the router.

Configuring the ISDN interface

This procedure is used if you are attaching the router to a PBX, changing the ISDN configuration.

1 To configure the ISDN interface, enter `network isdn2 configure`.

The router prompts as follows:

Note: This prompt may appear only if you are using Euro-ISDN.

```
Numbering plan identification <STANDARD or E163/4>
(STANDARD):
```

2 Do the following:

If you	Then
are attaching the router to a Siemens Octopus PBX	change the value to E163/4, so that the Siemens Octopus PBX can recognize the number plan the router is using.
are not attaching the router to a Siemens Octopus PBX	use the standard configuration.

The router prompts as follows:

```
Multiple subscriber numbering in use <YES or
NO> (no):
```

Network interface sub-context commands
configure (conf) (continued)

This allows several devices, such as telephones, faxes, routers, and so on, to be attached to one ISDN line but to have different numbers. Each device can then listen to all incoming calls on the line, but accept and reply only to calls sent directly to its individual number. Multiple Subscriber Numbering is only available from certain service providers.

3 Enter `yes` if you want to use Multiple subscriber dialing.

The router prompts as follows:

```
Self identification <YES or NO> (no):
```

If you enable this feature, the router provides its own ISDN number in outgoing calls.

4 Enter `NO`, as the network usually provides the calling ISDN number to the remote unit.

However, in some circumstances (especially when using a PBX), you would set this to `YES`.

The router prompts as follows:

Note: The following two prompts do not appear on all ISDN variants.

```
Generate high layer compatibility <YES or NO> (no):
```

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, Group 4 Fax, or is a video conference call, and so on.

5 Enter `YES` when the remote unit you are connecting 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 it will not work. The disadvantage of HLC is that it is not very common and you will probably find that you have to use Multiple Subscriber Numbering (MSN) or sub-addressing to achieve the same effect.

The router prompts as follows:

```
Check high layer compatibility <YES or NO> (no):
```

Network interface sub-context commands
configure (conf) (continued)

6 Enter YES if the router you are configuring is on an ISDN bus with multiple devices that can check for HLC.

The router prompts as follows:

```
Use keypad information element <YES or NO> (no):
```

If you are using National ISDN 1 or 2, enter yes to send dialed digits to the switch by the keypad; otherwise, enter no, to send dialed digits to the switch by the Called Party Number information element.

Note: If you find that your switch does not accept the dialed digits (for example, the dial tone does not switch off after you dial a digit) and you are not able to connect to a destination, then change your response to this prompt.

7 Respond as required.

The router prompts as follows:

```
Additional call offering <YES or NO> (no) :
```

Additional call offering allows you to pre-empt a data call by an analog call on a B-channel when both B-channels are in use.

Note: You can only use additional call offering if you have subscribed to this service offered by your service provider.

8 Choose yes to enable this feature.

The router prompts as follows:

Note: This prompt appears only if NI-1 has been chosen.

```
Strict NI-1 Conformance <YES or NO> (no) :
```

9 Enter no.

The router prompts as follows:

```
Remove TEI when cable disconnected <YES or NO>
(yes):
```

This option affects the way the HomeOffice Router re-establishes layer 2 communication with the ISDN PBX after the ISDN cable has been removed and then re-connected.

If you respond with yes, then whenever the HomeOffice Router detects that the cable has been reconnected, it assumes that all of the Terminal Endpoint Identifiers (TEIs) negotiated earlier are no longer valid and asks the PBX to assign new TEIs.

Network interface sub-context commands
configure (conf) (continued)

If you respond with no, the HomeOffice Router asks the PBX to verify that the TEIs it was using earlier are still valid. If the PBX instructs the HomeOffice Router to remove those TEIs, the HomeOffice Router attempts to negotiate new values.

Normally, you should respond with no to this prompt.

You should respond with yes if your ISDN service is provided by a Meridian PBX or if you are experiencing difficulties reconnecting after the cable is replaced.

Displaying ISDN interface configuration details

To display the current ISDN configuration, enter `network isdn2 configure show`.

A display similar to the following appears:

```
ISDN layers 2 and 3 configuration:

   ISDN connection type              : multipoint
   ISDN B Channels enabled           : 2
   Numbering plan identification     : e163/4
   Multiple subscriber numbering     : yes
   Self identification               : yes
   Generate high layer compatibility : yes
   Check high layer compatibility    : yes
   Additional call offering          : yes
```

Network interface sub-context commands

default (d)

Command purpose

The `network isdn2 default` command lets you see which users are using the default circuit configuration. Every WAN interface has a default circuit.

Command syntax

The syntax of the `default` command is as follows:

```
HomeOffice: network isdn2 default
```

Using the command

To determine who is using the default circuit values, enter `network isdn2 default`.

A display similar to the following appears:

```
Using Circuit Default Table

Name      Circuit Multilink  PPP  Security   Timer      Tune
default       n/a       n/a  n/a       n/a      n/a       n/a
listener      n/a       yes  yes        no      n/a       yes
user1          no       yes  yes        no      n/a       yes
radius        n/a       n/a  n/a       n/a      n/a       n/a
```

In the above display, `user1` is using the default circuit values for `Multilink`, `PPP`, and `Tune`.

Network interface sub-context commands

enabled (e)

Command purpose

The `network <interface> enabled` command allows you to enable or disable an interface. This command is available on all interfaces, working identically on each of them.

Command syntax

The syntax of the `enabled` command is as follows:

```
HomeOffice: network eth1 enabled [show]

HomeOffice: network isdn2 enabled [show]
```

Using the command

Note: This command affects only the current interface. To change another interface, enter it as a sub-context, and then use the `enabled` command there. You cannot specify another interface from the current interface.

Enabling or disabling an interface

1 To enable or disable an interface, enter `network <interface> enabled` where <interface> is either `eth1` or `isdn2`.

The router prompts as follows:

```
Enable interface <YES or NO> (no) :
```

2 Enter `yes` if you want to enable this interface or `no` if you want to disable it.

Any change you make does not take effect until you restart the router.

Network interface sub-context commands
enabled (e) (continued)

Displaying the status of all interfaces

To display the status of all interfaces, enter `network isdn2 enabled show.`

You see

```
                Interface Table

Interface          Enabled             Current
  eth1             yes                 enabled
=>isdn2            no                  disabled
```

Note: The => indicates the current context.

Network interface sub-context commands

multilink (m)

Command purpose

The `network isdn2 multilink` command lets you fine tune the PPP Multilink feature.

Command syntax

The syntax of the `multilink` command is as follows:

```
HomeOffice: network isdn2 multilink [show]
```

Using the command

Configuring PPP Multilink

1 To fine tune the PPP Multilink feature, enter `network isdn2 multilink`.

The router prompts as follows:

```
Circuit name <up to 15 characters or *> :
```

2 Type the name of the circuit on which you wish to carry out fine-tuning.

The router prompts as follows:

```
Use default circuit's configuration <YES or NO>
(yes):
```

3 Press <Enter> if you want your circuit to use the configuration of the default circuit.

No further prompts appear if you choose to adopt the default circuit's configuration.

The router prompts as follows:

```
Fragment packets <enabled or disabled> (enabled) :
```

If you set this option to ENABLED, PPP Multilink splits packets so that they are distributed in parallel down all channels in use. This reduces latency and speeds up data transmission. If you select ENABLED you can then specify the minimum size of packet to fragment.

Network interface sub-context commands
multilink (m) (continued)

4 Enter `enabled` if you want PPP Multilink to split packets.

The router prompts as follows:

```
Minimum size of packet to fragment
<128 - 1024> (256) :
```

5 Type the minimum size of packet that you wish to fragment.

The range is from 256 to 1024 octets.

Note: If you are experiencing frame loss, disable this option.

The router prompts as follows:

```
Generate NULL fragments <ENABLED or DISABLED>
(disabled): disabled
```

If you are experiencing packet loss, you can send NULL fragments to flush the receiver.

6 Type `enabled`. Otherwise leave this option `DISABLED` (the default value).

The router prompts as follows:

```
Omit encapsulation for single link <ENABLED or
DISABLED> (disabled):
```

If you set this option to `DISABLED`, PPP Multilink operates as normal. This means that each packet contains a multilink header, no matter how many links are open.

7 Set this option to `ENABLED` if you wish to omit multilink headers when only one link (the primary link) is open.

When the secondary link closes, packets retain headers for the purpose of synchronization before dropping them. This makes the packets smaller so that there is less data to send.

The following display shows the configuration you have set up:

```
Circuit updated:

   Circuit name                        : boston
   Fragment packets                    : enabled
   Minimum size of packet to fragment  : 256
   Generate NULL fragments             : disabled
   Omit encapsulation for single link  : disabled
```

Network interface sub-context commands
multilink (m) (continued)

Displaying the PPP Multilink configuration details

To display the multilink configuration, enter `network isdn2 multilink show`.

A display similar to the following appears:

```
Name      Fragment   Fragment   NULL       Suppress
          Packets    Size       Fragment   Headers

ISDN      n/a        n/a        n/a        n/a
admin     enabled    256        enabled    enabled
default   enabled    256        enabled    enabled
listener  n/a        n/a        n/a        n/a
ni1       enabled    256        enabled    enabled
```

Network interface sub-context commands

ppp (pp)

Command purpose

The `network isdn2 ppp` command is used to

- monitor the quality of throughput on a link, through the Link Quality Monitoring (LQM) function
- configure counters and timers used by PPP to maintain the integrity of negotiation sequences

Link Quality Monitoring Functions

The LQM function periodically sends packets to the target router, to check that the link is functioning correctly. You can enable or disable it.

You do not need to enable LQM. An ISDN line provides better quality communications than a standard leased line. You only pay for the time during which you use it. So LQM is probably redundant, and you can keep costs down by only using it when necessary.

Command syntax

The syntax of the `ppp` command is as follows:

```
HomeOffice: network isdn2 ppp [show]
```

Using the command

Configuring PPP

1 To configure PPP, enter `network isdn2 ppp`.

The router prompts as follows:

```
Link Quality Management <DISABLED or
ENABLED> (disabled):
```

The default value is `DISABLED`.

2 Enable or disable link quality management as required.

The router prompts as follows:

```
Echo request timer in seconds <1 - 10> (1) :
```

Network interface sub-context commands
ppp (pp) (continued)

3 Define how often PPP checks that the link is up.

The router prompts as follows:

```
Echo frames allowed to be lost <2 - 4> (2) :
```

4 Define the number of frames (or packets) that can be lost before PPP decides that the link is down.

The router responds as follows:

```
Ignore LCP Number Errors <YES or NO> :
```

5 Enter `no` if you want to ignore PAP authorization acknowledgment identification number errors. This may be required when using Layer 2 Forwarding (L2F) at the remote destination.

The router responds as follows:

```
Peer is Shiva Device <YES or NO> :
```

6 Respond as required.

The following prompts that appear are all checks on the time taken to negotiate links between the units.

```
Restart Timer in seconds <1-16> (3) :

Maximum Number of Configure-Requests
sent <1-10> (10):

Maximum Number of Configure-Naks sent
<1-5> (5):

Maximum Number of Terminate-Requests sent
<1 or 2> (2):
```

You should not change these values, as they are the default values for any router using the standard PPP setup. It is important that they be identical in both the original and target routers.

Network interface sub-context commands
ppp (pp) (continued)

Displaying PPP configuration details

To display the Circuit PPP Table for an interface, enter `network isdn2 ppp show`.

A display similar to the following appears:

```
Circuit PPP Table
Name  LQM      Restart Maximum   Maximum   Maximum  LCP
               Timer   Conf-Reqs Conf-Naks Term-Reqs State

HQ1  disabled   3        10         10        1       No VC
HQ2  disabled   3        10         10        1       No VC
Ad1  disabled   3        10         10        1       No VC
Ad2  disabled   3        10         10        1       No VC
```

The LCP State refers to the PPP Link Control Protocol which is used to negotiate default values for the following:

- encapsulation format options
- packet sizes
- peer identity authentication
- link quality monitoring

The value in the LCP State field varies, depending on the current state of PPP negotiation on that virtual circuit. Use `ppp show <circuit name>` to see detailed LCP state information.

Network interface sub-context commands

rates (rat)

Command purpose

The `network isdn2 rates` command provides continuous monitoring of the calls made and received by the router.

Command syntax

The syntax of the `rates` command is as follows:

```
HomeOffice: network isdn2 rates
```

Using the command

Setting the rates to monitor calls

To set rates for continuous monitoring, `enter network isdn2 rates <seconds>` where <seconds> is the frequency with which statistics are updated on screen. For example, `network isdn2 rates 5`.

The router responds with a display similar to the following:

```
Continuous monitoring of calls every 5 seconds. Enter
<Ctrl-C> to terminate.

Total Total Current Attempted Accepted Rejected Closed
in    out   in out  in  out   in  out  in out   in out
0     10    0  1    0   0     0   0    0  0     0   0
0     10    0  1    0   0     0   0    0  0     0   0
0     10    0  1    0   0     0   0    0  0     0   0
0     10    0  1    0   0     0   0    0  0     0   0
```

To stop the display, press <Ctrl-C>.

For details about calls made to a particular destination, enter `network isdn2 rates`, followed by the destination name or address.

Network interface sub-context commands
rates (rat) (continued)

Displaying call monitoring information

For details about calls made on a particular circuit, enter `network isdn2 rates`, followed by the circuit name and number of seconds.

For example, `network isdn2 rates nortel1 5`

You see

```
Continuous monitoring of VCs every 5 seconds.
Enter <Ctrl-C> to terminate.
    --- Packets sent ---          ---- Packets received ----
VCs Total Pkt Oct Protocol(%)     Total Pkt Oct Protocol(%)
    sent  /s   /s  IP IPX OSI BR rec'd /s /s  IP IPX OSI BR
1   6977  3  1543  100  0   0  0 6907  3  1543 100 0   0  0
1   6993  3  1589  100  0   0  0 6922  3  1543 100 0   0  0
1   7023  3  1543  100  0   0  0 6952  3  1543 100 0   0  0
```

To stop the display, press <Ctrl-C>.

Network interface sub-context commands

rejects (rej)

Command purpose

The `network isdn2 rejects` command displays information about incoming calls rejected by the router and outgoing calls that the router has failed to make.

Information about rejected incoming calls is particularly useful if you have two routers that cannot communicate across the ISDN WAN, as it shows the address of the station that made the rejected call.

Information displayed about rejected outgoing calls does not include calls made or received using the `isdn2 test` command.

Command syntax

The syntax of the `rejects` command is as follows:

```
HomeOffice: network isdn2 rejects in

HomeOffice: network isdn2 rejects out
```

Using the command

Displaying rejected incoming calls

To display a list of rejected incoming calls, enter `network isdn2 rejects in`.

You see

```
                Incoming Rejects

Address     Failures  Time Since    Cause
                      Last Reject
0315549123      1     13h 28m       call rejected
personnel       3     1h  3m        call timed out
listener        4     2m  10s       PAP not authenticated
```

Network interface sub-context commands
rejects (rej) (continued)

If the router can make an association between the address used and a circuit name, it uses the circuit name in the display. If it cannot, it displays the address. In this case, you need to check the relevant circuit table and correct the entry.

Displaying rejected outgoing calls

To display a list of rejected outgoing calls, enter `network isdn2 rejects out`.

The display that appears is very similar to the list of rejected incoming calls.

Check that the ISDN address received in the ISDN Circuit table matches this address. (Use `ip isdn2 association show` command.) If it does not, change the address in the Circuit table. This lets the router accept calls from this address.

Network interface sub-context commands

security (sec)

Command purpose

When the Point-to-Point Protocol (PPP) is used on the router, security must also be used. The Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Shiva Password Authentication Protocol (SPAP) are the security mechanisms for PPP.

PAP, CHAP, and SPAP check the identity of a caller, as an alternative to the Calling Line Identification (CLI) feature.

Note: Caller ID is the North American equivalent of CLI.

CLI is not always implemented, particularly on international calls. PAP, CHAP, or SPAP can also be used in addition to CLI.

The `network isdn2 security` command is used to enable or disable PAP, CHAP, or SPAP on the router.

Command syntax

The syntax of the `security` command is as follows:

```
HomeOffice: network isdn2 security
```

Using the command

Enabling security

1 To enable PAP, CHAP, or SPAP on the router, enter `network isdn2 security`.

The router prompts as follows:

```
Circuit name <Up to 15 characters or *> :
```

2 Select the circuit for which you want to activate PAP, CHAP, or SPAP.

The router prompts as follows:

```
Authentication <DISABLED, PAP, CHAP or SPAP> (chap)
:
```

Network interface sub-context commands
security (sec) (continued)

3 If authentication is not required, enter DISABLED.

To enable authentication, enter PAP, CHAP, or SPAP.

The following table identifies where to find instructions for the authentication method you have chosen.

For	See
CHAP	“Enabling CHAP” on page 7-57
PAP	“Enabling PAP” on page 7-58
SPAP	“Enabling SPAP” on page 7-60

Enabling CHAP

```
My CHAP Identifying name <up to 48 characters or
NONE> (none) :
```

1 Enter an identifying name for the router you are configuring, such as its ISDN address.

Note: You must configure the listener circuit's identifying name if you want to use CHAP.

The router prompts as follows:

```
Their CHAP Identifying name <up to 48 characters or
NONE> (none) :
```

2 Enter a unique identifying name for the device at the other end of the circuit.

On an ISDN circuit, if you have set the Address Received to `NULL`, then this prompt appears as `not assigned`. You must enter an Identifying name. However, if you have entered an ISDN Received Address, the default `NONE` is an acceptable value.

The router prompts as follows for shared secrets on both the router (for incoming challenges) and the device at the remote site (for outgoing challenges).

```
New shared secret <up to 25 characters or NONE> :
Repeat new shared secret <up to 25 characters or
NONE> :
```

These additional identifiers are actually passwords for the router you are configuring. To be effective, they should differ from the identifying names entered above.

3 Enter the router's secret.

Note: The shared secret is not echoed on screen. Be careful to take note of what you have entered here and keep this information in a safe place.

4 Retype the secret to confirm that you have typed it correctly.

5 Repeat steps 3 and 4 for the remote device's secret.

The router prompts as follows:

```
Simultaneous 2-way Authentication <YES or NO> (no):
```

6 If you want both incoming and outgoing challenges to be authenticated at the same time, enter YES.

The new circuit details appear.

```
Circuit updated:

  Circuit name                        : nortel1
  Authentication                      : chap
  Use default circuit's configuration : n/a

CHAP parameters:
  My identifying name                 : 3939
  Their identifying name              : 2929
  Two way authentication              : no
```

Enabling PAP

The same parameter values must be defined in reverse on the router on the other side of the circuit.

The router prompts as follows:

```
My PAP Peer ID <Up to 48 characters or
NONE> (NONE) :
```

Network interface sub-context commands
security (sec) (continued)

1 Enter a Peer ID for the router you are configuring, such as its ISDN address.

The router prompts as follows:

```
Their PAP Peer ID <up to 48 characters or NONE>
(NONE):
```

2 Enter a unique Peer ID for the device at the other end of the circuit.

On an ISDN circuit, if you have set the Address Received to `NULL`, then this prompt appears as `not assigned`. You must enter a PAP Peer ID. However, if you have entered an ISDN Received Address, the default `NONE` is an acceptable value.

The router prompts as follows:

```
My PAP Password <Up to 15 characters or
NONE> (NONE) :
```

This is an additional identifier. To be effective, it should differ from the Peer ID.

3 Enter a password for the router you are configuring.

The router prompts as follows:

```
Their PAP Password <Up to 15 characters or NONE>
(NONE):
```

4 Enter a PAP password for the device at the other end of the circuit.

The new circuit details appear.

```
Circuit updated:

  Circuit name                        : trial1
  Authentication                      : pap
  Use default circuit's configuration : n/a

PAP parameters:
  My    PAP peer ID                   : bill
  Their PAP peer ID                   : ted
  My    PAP password                  : <none>
  Their PAP password                  : <none>
```

Network interface sub-context commands
security (sec) (continued)

Enabling SPAP

The router prompts as follows:

```
Return ISDN address <up to 41 digits or NULL>
NULL) :
```

1 Enter the ISDN directory number of your HomeOffice Router.

This directory number will be used by the remote device to connect to your HomeOffice Router.

The router prompts as follows:

```
My SPAP Peer ID <Up to 48 characters or NONE>
(NONE):
```

2 Enter a Peer ID for the router you are configuring.

This is the router's ISDN address or the name of the site in which it is located for each circuit.

The router prompts as follows:

```
Their SPAP Peer ID <up to 48 characters or
NONE> (NONE):
```

3 Enter a unique Peer ID for the device at the other end of the circuit.

The router prompts as follows:

```
My SPAP Password <up to 16 characters or
NONE> (NONE):
```

This is an additional identifier. To be effective, it should differ from the Peer ID.

4 Enter a password for the router you are configuring.

Note: SPAP passwords are encrypted, so they are not echoed on screen.

The router prompts as follows:

```
Repeat new password <up to 16 characters>:
```

Network interface sub-context commands
security (sec) (continued)

5 Type the password again as confirmation.

The router prompts as follows:

```
Their SPAP Password <Up to 16 characters or
NONE> (NONE):
```

6 Enter a password for the device at the other end of the circuit.

The router prompts as follows:

```
Repeat new password <up to 16 characters>:
```

7 Type the password again as confirmation.

The new circuit details appear.

```
Circuit updated:

  Circuit name                        : trial1
  Authentication                      : spap
  Use default circuit's configuration : n/a

SPAP parameters:
  Return ISDN address                 :5551234
  My SPAP peer ID                     : bill
  Their PAP peer ID                   : ted
```

Displaying authentication configuration details

To display the circuit security table, enter `network isdn2 security show`.

A display similar to the following appears:

```
Circuit Security Table

Circuit  Auth  My Id      Their Id  Warning
admin    pap   SAP100000  <none>    -
default  spap  123                   -
listener all   n/a                   -
voice          n/a         n/a
```

Network interface sub-context commands
security (sec) (continued)

This shows the circuits that have PAP, CHAP, or SPAP enabled. It also shows details of the listener circuit. The listener circuit is used where there is no Calling Line Identification (CLI). When a router receives a call, the calling address will be seen as NULL if CLI is disabled. The listener circuit is then used to carry out the PPP negotiation until the real circuit is established.

If PAP is in use on your network, the Peer ID is checked against the circuit table at the other end of the network, to see if a circuit is set up for that address.

If CHAP is in use on your network, my identifying name (set in the listener circuit) is checked against the circuit table at the other end of the network, to see if a circuit is set up for that address.

Network interface sub-context commands

statistics (ss)

Command purpose

The `network eth1 statistics` command displays frame and packet statistics for a specific interface.

You can also display rates, discards, and errors, or reset the statistics counter.

Command syntax

The syntax of the `statistics` command is

```
network eth1 statistics <modifier>
```

where `<modifier>` can be `frames`, `rates`, `discards`, `errors queue`, or `reset.`

Using the command

Displaying transmitted and received frames

To display frames that have been received and transmitted, enter `network eth1 statistics frames`.

A display similar to the following appears:

Network interface sub-context commands
statistics (ss) (continued)

```
Interface Statistics: eth1

 Total frames received      :   16487 (100.00%)
    Protocol frames         :       0 (  0.00%)
    Bridged frames          :     303 (  1.83%)
    Media control frames    :       0 (  0.00%)
    Discards                :   16183 ( 98.15%)
    Errors                  :       1 ( 00.00%)

 Total octets received      :  4414470(avg frame size 267)

 Total frames transmitted   :     161 (100.00%)
    Protocol frames         :       0 (  0.00%)
    Bridged frames          :     158 ( 98.13%)
    Media control frames    :       0 (  0.00%)
    Discards                :       3 (  1.86%)
    Errors                  :       0 (  0.00%)

 Total octets transmitted   :   23166(avg frame size 146)

 Total media transmit errors :     1
```

Displaying transmit and receive rates

To display transmit and receive rates by the router, enter `network eth1 statistics rates`.

A display similar to the following appears:

Network interface sub-context commands
statistics (ss) (continued)

```
Interface Statistics: eth1

                        Peak                    Current

Total received      :  398 pps   (  6m 47s)    83 pps
    Protocol frames :    0 pps                  2 pps
    Bridged frames  :    0 pps                  1 pps
    Media control   :    0 pps                  0 pps
    Discards        :  398 pps   (  6m 47s)    80 pps
    Errors          :    0 pps                  0 pps

Receive data rate   :88306 bps   ( 5m 23s) 105000 bps

Total transmitted   :    3 pps   ( 17m 34s)     1 pps
    Protocol frames :    0 pps                  0 pps
    Bridged frames  :    3 pps   ( 17m 34s)     1 pps
    Media control   :    0 pps                  0 pps
    Discards        :    0 pps                  0 pps
    Errors          :    0 pps                  0 pps

Transmit data rate  : 3890 bps   ( 17m 14s)   916 bps
```

Displaying transmit and receive discards

To display discarded transmissions and receipts, enter `network eth1 statistics discards`.

A display similar to the following appears:

```
Interface Statistics: eth1

 Total receive discards      :      31295 (100.00%)
    Interface down           :          0 (  0.00%)
    Unrecognized protocol    :         45 (  0.14%)
    Filtered dynamically     :      29357 ( 93.80%)
    Filtered statically      :          0 (  0.00%)
    Port not forwarding      :       1893 (  6.04%)

 Total transmit discards     :          3 (100.00%)
    Interface down           :          2 ( 66.66%)
    Unrecognized protocol    :          0 (  0.00%)
    Filtered dynamically     :          0 (  0.00%)
    Filtered statically      :          0 (  0.00%)
    Port not forwarding      :          1 ( 33.33%)
```

Displaying transmit and receive errors

To display transmit and receive errors, enter `network eth1 statistics errors`

A display similar to the following appears:

```
Interface Statistics: eth1

Total receive errors        :          5 (100.00%)
   Resource                 :          5 (  0.00%)
   Stream                   :          0 (  0.00%)
   Receive                  :          0 (  0.00%)
   Overrun                  :          0 (  0.00%)
   Frame check sequence     :          0 (  0.00%)

Total transmit errors       :          0 (  0.00%)
   Resource                 :          0 (  0.00%)

Total media transmit errors :          2
   Transmit                 :          0
   Collision                :          2
```

Network interface sub-context commands
statistics (ss) (continued)

To display information about the transmit and receive queues on the router, enter `network eth1 statistics queue`.

A display similar to the following appears:

```
Interface Statistics: eth1

Receive queue
    Max Driver buffers       :        100
    Current Driver buffers   :        100 (100.00%)

Transmit queue
    Max Driver buffers       :         50
    Current Driver buffers   :         50 (100.00%)
    Tx queue size (frames)   :          0

 Interface driver-to-streams queue
    Protocols                : Xerox echo,
    Read queue size          :          0
    Protocols                : Bridge,
    Read queue size          :          0

 Bridge driver-to-streams queue
    Protocols                : Spanning Tree, Bridge
    Read queue size          :          0
```

Resetting the statistics counter

To reset the statistics counter, enter `network eth1 statistics reset`.

Network interface sub-context commands

status (st)

Command purpose

The `network <interface> status` command displays information about the physical status of the network connection. It is available on Ethernet and ISDN interfaces.

Command syntax

The syntax of the `status` command is as follows:

```
HomeOffice: network eth1 status

HomeOffice: network isdn2 status
```

Using the command

To display the status of the network connection, enter `network <interface> status`, where <interface> is either `eth1` or `isdn2`.

The Ethernet display looks like this:

```
Interface Status:

Interface number   : 1
  Current State    : up
  Duration         : 17m  1s
  Type             : ethernet
  Variant          : auto
  Bandwidth (bps)  : 10000000
System name        : eth1
  Alias            : local
Requested State    : enabled
```

Network interface sub-context commands

test (te)

Command purpose

The `network isdn2 test` command is used to test

- ISDN without the full configuration procedure
- a configured line that is suspected of being faulty

Loopback test

The first test you should run is the loopback test which verifies

- that the unit can communicate with the ISDN exchange (that is, the cable and interface card are working)
- that the number the telephone company has actually assigned (the ISDN number of the local ISDN connection) and the number you think you have are the same
- whether CLI is installed on your line
  If it is, the loopback tests if the exchange inserts any extra digits in the CLI. This may affect how you configure the unit for communication.
- the data path to and from the ISDN exchange
- SPIDs if you are using National ISDN (North America only).

Note: The loopback test is not available on an ISDN line that is provisioned for only one B-channel.

Listening and calling tests

After you have successfully completed the loopback test and are confident that connections and addresses are correct, you can test the ability of two routers to connect over ISDN. Use the `LISTEN` and `CALLING` test options. Set up one unit to listen and the other to call.

Note: You must run this test in co-operation with someone at the other end of the ISDN link. One end of the link is called the Listening Side; the other end is the Calling Side.

Reversing the listening and calling tests

Upon completion of the listening and calling tests, reverse the listening and calling states of the routers and run the test again.

> ***Note:*** It is important to run the test in reverse. Even though the test works in one direction, this does not mean that the numbers are correct in the opposite direction. Most networking protocols require that either end can initiate the call.

If the tests are unsuccessful, do the following:

- Try the loopback test again.
- Contact the telephone company and check that you are using the correct area codes at both ends.

Command syntax

The syntax of the `test` command is as follows:

```
HomeOffice: network isdn2 test
```

Using the command

Performing a loopback test

1 To run a loopback test, enter `network isdn2 test.`

The router responds as follows:

```
Entering TEST mode on ISDN interface:
(CTRL-C to exit)

Select test mode <LISTEN, CALLING or
LOOPBACK> (loopback) :
```

Network interface sub-context commands
test (te) (continued)

2 Select `loopback`.

This is the default (shown in parentheses), so you only need to press <Enter>.

The router prompts you for the following:

```
ISDN address to dial this interface <up to 41
digits> (NULL):
```

Note: The default value is NULL, or the number that you entered for this unit using the `install` command or the `network isdn2 address` command. In most cases, you will not want to change a number that you have previously entered.

If you wish to test a sub-address, you can add it here.

3 Enter the ISDN interface address, then a hyphen followed by the sub-address number.

For example, if the number you want the router to listen for is 0123 555 2001, with a sub-address of 2, you would do the following:

a. Enter it as an ISDN interface address. For example, `01235552001`.

b. Enter a hyphen and a digit as a sub-address. For example, `-2`.

The complete address is 01235552001-2.

By adding the last digit after the sub-address separator (hyphen), you tell the router what sub-address digit to listen for in incoming calls. Sub-addresses can be more than one digit.

c. Press <Enter>.

The router reports the ISDN calls it sees coming in, not going out. If it sees nothing, it reports that the loopback test has failed. If the router receives a call, but does not recognize that this call was its own call to itself, the test fails. The following describes the possible reasons for this failure.

Loopback test failure

The possible reasons for failure are:

- The ISDN network has not identified the router because Calling Line Identification (CLI) is not supported on your network. If this is the case, you will get the result `Incoming Call from NULL`. You should use the `install` command to configure circuits with `NULL CLI`, and use PAP or CHAP to identify the calling unit, or use `net isdn2 circuit change` and `net isdn2 security`.
- The ISDN network has identified the router incorrectly because the ISDN network has added an area code prefix to the number. For example, you will get the result `Incoming Call from 0101234567890`. In this case, retry the test. At the `Network Identification Address` prompt, you should enter the full number, including the prefix, as reported by the loopback test.
- Another user tried to call you as you were carrying out the loopback call and nullified the test. You should repeat the test.

Troubleshooting the loopback test

If the loopback test fails for any other reason, you should check

- the ISDN cable
- the ISDN interface
  Enter `status` to make sure it is up. If it is not, check it using the `top fault` command.
- the ISDN number
  To do this, contact your ISDN supplier.
- the ACT LED on the ISDN interface card
  If this does not shine green, then the ISDN link to the network is down. This may be due to a problem with either the cable, the router, or the ISDN exchange. It indicates that the problem is not simply a numbering one.

Network interface sub-context commands
test (te) (continued)

Performing Listening and calling tests

At the listening side, do the following:

1 Go into the `network isdn2` context and type `network isdn2 test`.

The router prompts with the following:

```
Entering TEST mode on ISDN interface: <CTRL-C to
exit>
Select test mode <LISTEN, CALLING or LOOPBACK>
(loopback):
```

2 To check that the router can receive calls, type `listen`.

The router prompts with the following:

```
ISDN directory number of this interface <up to 41
digits> (1234567890):
```

3 Select the default by pressing <Enter>.

The default is the address set up in the `isdn2 address` command. However, any address can be used here. If you wish to test a sub-address, enter that address.

```
Automatically Accept All incoming calls <MANUAL or
 AUTO> (auto):
```

Note: If you select `AUTO` (the default value), the router accepts all calls. If you select `MANUAL`, the router asks if you want to accept specific calls.

```
Listening for incoming calls . . . . .
```

Note: The router indicates that it is in a listening state, adding a dot to the line every four seconds.

At the calling side, do the following:

4 On the router at the other end of the ISDN link, type `network isdn2 test`.

5 Select the `CALLING` test option.

The router responds as follows:

```
ISDN number to call <up to 41 digits>:
```

6 Enter the ISDN address of the listening unit and press <Enter>.

Effects at the listening side

If you have elected to accept incoming calls manually, the router at the listening end asks if you want to accept a specific call in the following way:

```
Call received from 1234567890.
Accept this incoming call <NO or YES> :
```

If you have elected to accept incoming calls automatically, you will see the following:

```
Call received from 1234567890.
Automatically accepting call

Incoming call state : LISTENING -> ACCEPTING
Incoming call state : ACCEPTING -> ESTABLISHED
Message received:  This message was sent on the
B-channel
```

The call is closed automatically once the test message has been received.

```
Incoming call state: ESTABLISHED -> LISTENING
Listening for incoming calls . . . . . .
```

The listening router indicates that it is again in a listening state, adding a dot to the line every four seconds.

Effects at the calling side

The calling unit displays the following if the test is successful:

```
Outgoing calling state:  ATTEMPTING -> CONNECTING
Outgoing calling state:  CONNECTING -> ESTABLISHED

Call connection was successful.
```

If the test is unsuccessful, press <Ctrl-C> to exit and then retry the test.

Network interface sub-context commands

timer (ti)

Command purpose

The `network isdn2 timer` command is used to define the intervals at which the router attempts to back up or open an ISDN circuit that is down.

Command syntax

The syntax of the `timer` command is as follows:

```
HomeOffice: network isdn2 timer
```

Using the command

1 To configure the timers, enter `network isdn2 timer`.

The router prompts as follows:

```
Circuit name <up to 15 Characters or *> :
```

2 Enter the name of the circuit for which you want to configure the timer.

The router prompts as follows:

```
Use default circuit's configuration <YES or NO>
(yes) :
```

3 Press <Enter> if you want your circuit to use the configuration of the default circuit.

No further prompts appear if you choose to adopt the default circuit's configuration.

The router prompts you to enter the backup timer retry method.

```
Backup timer retry method <EXPONENTIAL, LONG or
SHORT> (exponential) :
```

Network interface sub-context commands
timer (ti) (continued)

The options are described in the following table:

Retry method	Description
Exponential	This sets the timer to retry at the short interval (30 seconds) for a few attempts. This interval is increased until it reaches the long interval (1200 seconds).
Long	This sets the timer to repeat attempts to open a circuit at intervals of 1200 seconds.
Short	This sets the timer to repeat attempts to open a circuit at intervals of 30 seconds.

4 Select the retry method.

The router prompts you to enter the circuit down timer retry method.

```
Circuit down timer retry method <EXPONENTIAL, LONG
or SHORT> (exponential) :
```

The new values appear.

```
Circuit updated:

Circuit name                        : trialci1
 Backup timer retry method          : long
 Circuit down timer retry method    : exponential
Use default circuits configuration  : disabled
```

Network interface sub-context commands

tune (tu)

Command purpose

The `network isdn2 tune` command lets you change circuit parameters on an individual basis. It is available in `isdn2` sub-contexts.

> ***Note:*** You must set Bandwidth-on-demand criteria for increasing and decreasing bandwidth at both ends of a link.

Command syntax

The syntax of the `tune` command is as follows:

```
HomeOffice: network isdn2 tune
```

Using the command

1 To change circuit parameters on an ISDN interface, enter `network isdn2 tune`.

The router prompts as follows:

```
Circuit name <up to 15 characters or *> :
```

2 Select the circuit you want to tune.

The router prompts as follows:

```
Use default circuit's configuration <YES or NO>
(yes) :
```

3 Press <Enter> if you want your circuit to use the configuration of the default circuit.

No further prompts appear if you choose to adopt the default circuit's configuration.

The router prompts as follows:

```
Circuit mode <PERMANENT or DEMAND> (demand) :
```

4 Select the circuit mode.

You should normally select `DEMAND`. `PERMANENT` keeps the link open all the time and prevents it from being preempted. Only select it if you have arranged with your telephone company to be on an appropriate ISDN Tariff.

The router prompts as follows:

```
Circuit priority <HIGH, MEDIUM or LOW> (low) :
```

Network interface sub-context commands
tune (tu) (continued)

5 Define whether calls on this circuit have a `HIGH`, `MEDIUM`, or `LOW` priority.

If all resources are in use, a call can pre-empt 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 pre-empted. (If priorities are equal, see the `Guaranteed call time in seconds` prompt.)

The router prompts as follows:

```
Minimum call timer in seconds <0 - 3600> (10) :
```

6 Define the minimum time, in seconds, that you want the specified circuit to be kept open.

You should set this to just less than the length of time of the minimum call unit set by your telephone company. This means that the circuit is configured to be kept open for at least the minimum time for which you are paying.

The router prompts as follows:

```
Call idle timer in seconds <2 - 3600 or
INFINITY> (10) :
```

7 Define how long a connection can remain idle before the router closes it down.

Change this if you don't want to use the default value that you set using the `timer` command. Set a value between `1` and `3600` seconds, or `INFINITY`. If you choose `INFINITY`, connections on this circuit will never time out.

Setting the value for the connection idle timer too low, especially on links with long connection setup times, can result in a connection always timing out before it is properly established.

Network interface sub-context commands
tune (tu) (continued)

The router responds as follows:

If the circuit is	Then
a PBX circuit (Meridian)	no further prompts appear. Instead the updated circuit details appear.
a voice or data circuit	the following and additional prompts appear: `Pre-emption timer in seconds <1-43200 or INFINITY> (60):` Continue with the rest of this procedure.

8 Define how long a connection can be open before it can be pre-empted by another call, unless the other call has a higher priority. If you enter `infinity`, the connection can never be pre-empted other than by a call with a higher priority.

The router prompts as follows:

```
Max. number of virtual circuits <1 or 2> (1):
```

9 Define the maximum number of virtual circuits that this circuit can carry.

This lets you use more than one virtual circuit to reach a destination, which can improve line use. If you do this, call prioritization may not work as described above.

Note 1: When you are using one virtual circuit per destination, a call can only pre-empt another if it has a higher priority.

Note 2: When you are using multiple virtual circuits, the effective priority is lowered to stop calls to a particular destination from monopolizing resources. For example, a low priority call can pre-empt one of the virtual circuits being used by a medium priority call, if the medium priority call is using two or three virtual circuits.

If all available logical channels are in use, incoming calls cannot pre-empt them because the network does not forward the call request to the router. Outgoing calls can pre-empt one circuit at a time.

Network interface sub-context commands
tune (tu) (continued)

The router prompts as follows:

```
Circuit Usage Thresholds -SNMP trap if exceeds
  Max single call length in minutes <1 - 9999 or
  INFINITY> (180) :
```

This lets you set a maximum limit for the length of an ISDN call (in minutes). If this limit is exceeded, an SNMP trap is sent.

10 Enter the number of minutes to which ISDN calls are limited.

The router prompts as follows:

```
Max daily percentage of available bandwidth
<1 - 99 or INFINITY> (35) :
```

This lets you set a maximum daily percentage of available bandwidth to be used for calls. The value you set for this should take into account the number of virtual circuits you have available. For example, if you have two virtual circuits 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.

Note: The above prompts only set the limits at which you are warned about excessive use of bandwidth, if you enable the relevant SNMP traps using the `traps` command. They do not alter the configuration being used.

The traps for both these thresholds can be enabled using the `snmp traps` command.

11 Enter a percentage to which daily bandwidth is limited.

The router prompts as follows:

```
Bandwidth on Demand - Criteria for increasing
bandwidth
Bandwidth on Demand management <CALLER or BOTH>
(both):
```

Network interface sub-context commands
tune (tu) (continued)

12 Do the following:

If	Then
you are using two routers	both ends of the link should use the same setting.
you are interoperating with another vendor's device	select CALLER.

The router prompts as follows:

```
Increase bandwidth on traffic burst <YES
or NO> (yes):
```

13 Respond as required.

If	Then
you enter yes at this prompt	a new virtual circuit is opened and data is transferred onto it if a sudden burst of data occurs.
you enter no	data transmission remains only on the existing virtual circuit during a sudden burst.

The router prompts as follows:

```
Increase bandwidth on sustained traffic load <YES
or NO> (yes) :
```

Network interface sub-context commands
tune (tu) (continued)

14 Respond as required.

If	Then
you enter `yes`	an additional virtual circuit is opened and data is transferred onto it when the volume of data on the existing virtual circuit exceeds the threshold value for a set length of time.
you enter `no`	data transmission remains on the existing virtual circuit.

Note: You must answer `yes` to at least one of the previous two prompts, otherwise the secondary circuit will never be opened.

The router prompts as follows:

```
Traffic load percentage <0 - 100> (80) :
```

This prompt appears only if you answered `yes` to the `Increase bandwidth on sustained traffic load` prompt. When data transmission on the existing virtual circuit reaches this level and remains there for the specified time (see following prompt), additional virtual circuits open for data.

15 Enter the traffic load percentage.

The router prompts as follows:

```
Required load duration in seconds <5 - 60> (5) :
```

This prompt appears only if you answered `yes` to the `Increase bandwidth on sustained traffic load` prompt.

16 Define the length of time for which data must reach (or exceed) the traffic load percentage value.

For example, when using the default values, the secondary circuit is opened up once traffic on the primary circuit has remained at or above the threshold of 80% for five seconds.

The router prompts as follows:

```
Threshold for decreasing bandwidth
  Traffic load percentage <0 - 40> (30) :
```

Network interface sub-context commands
tune (tu) (continued)

17 Enter the traffic load percentage.

When data transmission on the existing virtual circuit falls below this level for a sustained length of time (see following prompt), the number of virtual circuits is reduced.

The router prompts as follows:

```
Required load duration in seconds <5 - 60> (10) :
```

This is the length of time for which data must fall below the traffic load percentage value. For example, if you keep the default values, the secondary circuit automatically closes down when its data levels have fallen below the threshold of 30% for 10 seconds.

18 Enter the load duration in seconds.

The new details of the circuit appear.

Displaying circuit configuration details

To display the circuit parameters, enter `network isdn2 tune show`.

The display similar to the following appears:

```
Circuit Tuning Table
Name      Priority  Call  Idle  Pre-empt  VCs   BOD    BOD    Warning
                    Timer Timer Timer           Burst  Sustain
Dallas    low       90    60    90        1     yes    yes        -
Meridian  high      90    60    -         1     -      -          -
default   low       10    10    60        1     yes    yes        -
listener  low       10    10    60        1     yes    yes        -
voice     high      -     -     -         2     -      -          -
```

Note: If a warning is shown, enter `tune show <circuit name>` for more information.

Network interface sub-context commands

vcs (v)

Command purpose

The `network isdn2 vcs` command is used to display general statistics about the router's virtual circuits. It is available in all `isdn2` sub-contexts.

Command syntax

The syntax of the `vcs` command is as follows:

```
HomeOffice: network isdn2 vcs
```

Using the command

To display statistics about virtual circuits, enter `network isdn2 vcs`.

A display similar to the following appears:

```
WAN VC Statistics

Remote   VC  Call State    Duration  Packets  Packets
 router                               in       out

P integ-1  1  out  Transfer  32m 50s  5919     5973
=>integ-2  3  out  Transfer  17m 31s  3214     4123
```

All of the statistics given apply to calls the router is currently making. There is one line for each virtual circuit in operation.

Displaying statistics for a specific circuit

To display more details about calls to a particular destination, enter `network isdn2 vcs` followed by the circuit name.

A display similar to the following appears:

```
VC   Call  State    Duration  T/O idle(s)  T/O Preempt(s)
1    out   Transfer 33m5s     Infinity     Infinity
VC 1      Transmitted     rate/s    Received        rate/s
Packets   6019             3        5964             3
IP        6019(100.00%)    3        5964(100.00%)    3
Octets    3053395          538      3038356          1530
IP        3053395(100.00%) 1538     3038356(100.00%) 1530
```

SNMP context shell commands

The `snmp` context lets you manage all SNMP functions.

In the `snmp` context, the command prompt is

```
HomeOffice: snmp
```

The following commands are described in this chapter:

Command	Shortcut	Description
community	com	Add, change, delete, or show SNMP community names.
manager	m	Add, change, delete, or show SNMP managers.
traps	tra	Change or show SNMP traps.
validate	v	Validate SNMP managers and communities.

To display a list of available commands, enter `help`. To exit back to non-privileged level, enter `quit`.

community (com)

Command purpose

The SNMP `community` command operates on the SNMP Community table.

A community is a group of central management stations that can all manage the same equipment. In the SNMP protocol, communities are defined. Each community has a community name, which is stored in the Community table.

Command syntax

The syntax of the `community` command is as follows:

```
HomeOffice: snmp community <action>
```

where `<action>` is either `add`, `change`, `delete`, or `show`.

Using the command

The router can be managed from any SNMP management station. The Community table acts as a filter on incoming SNMP requests. It contains a list of the communities that are allowed access to manage the router. Each community is given one of two levels of access:

Access level	Description
`none`	Stations in this community have no access to the router.
`read`	Stations in this community may view the router 's parameters and statistics, but they cannot change the configuration.

Note: The Community table only acts as a filter if you switch on filtering. To do this, use the `validate` command.

The router can deal with up to eight communities. By default it has two, called `public` and `private`.

community (com) (continued)

Adding communities

1 To add an SNMP community to the community table, enter `snmp community add`.

The router responds as follows:

```
SNMP community name <up to 16 characters> :
Access permission <NONE or READ> :
```

2 Enter the appropriate values for your system.

For details on how to set up communities, see your management station's documentation.

Before you set an access permission to `none`, ensure you do not exclude your own management station by mistake.

Changing communities

To change a community, enter `snmp community change.`

The prompts are the same as for `community add`. To keep an existing value, press <Enter>.

Deleting a community

To delete a community table entry, enter `snmp community delete` followed by the name of the community you want to delete. If you do not specify a community name in the command, the router prompts for one.

The router displays the entry and asks you to confirm that you want to delete it.

```
Community name : beta
Access permission : read
Delete SNMP level entry <YES or NO> :
```

The router does not delete the community until you enter `yes`.

community (com) (continued)

Displaying communities

To display the SNMP community access table, enter `snmp community show`.

The following appears:

```
SNMP Community Access Table

      Community            Access
      public               read
      finance              none
```

manager (m)

Command purpose

The `snmp manager` command operates on the SNMP Manager table. Assuming that filtering is switched on (using the `validate` command), the Manager table acts as a filter on incoming SNMP requests, so that only management stations in the table can change the router 's configuration. Other management stations still have access to statistics and information.

Command syntax

The syntax of the `manager` command is as follows:

```
HomeOffice: snmp manager <action>
```

where `<action>` is either `add`, `change`, `delete`, or `show`.

Using the command

Adding a manager entry

1 To add an entry to the Manager table, enter `snmp manager add`.

The router prompts as follows:

```
SNMP manager <Internet address> :
```

2 Enter the Internet address or name of the central management station to which you want to give router access.

The router prompts as follows:

```
Send traps to manager <YES or NO> (yes) :
```

The default value (`yes`) causes the router to forward any SNMP trap messages to the central management station. You can set up traps with the `snmp traps` command. You should only send traps to management stations that can make use of them.

For security reasons, you may not wish to send traps to insecure devices. You may also decide not to send traps to some devices in order to avoid unnecessary network traffic.

3 Enter `yes` or no as required.

The router prompts as follows:

```
Send syslog messages to manager YES or NO (no) :
```

manager (m) (continued)

4 Enter YES if you want to send trap messages to a syslog daemon.

The router prompts as follows:

```
SNMP Community Name Up to 16 characters (public) :
```

5 Enter the community name to include in SNMP trap messages.

Changing a manager entry

To change an existing entry in the Manager table, enter `snmp manager change`.

The prompts are the same as for `manager add`. To keep the existing value, press <Enter>.

You can enter `*` when the router prompts for an Internet address, to display a list of the Internet addresses in the Manager table.

Deleting a manager entry

To delete an entry from the Manager table, enter `snmp manager delete` followed by the management station's Internet address.

If you do not enter the management station's Internet address in the command, the router prompts you for it.

The router displays the entry for that address and asks you to confirm that you really want to delete it.

Displaying manager entries

To display the Manager table, enter `snmp manager show`.

The following appears:

```
        Snmp Management Station Table

  Manager    Send Traps   Send Syslog   Community Name

31.0.0.11       yes           no           public
31.0.0.12       yes           no           private
31.0.0.13        no           no           public
```

manager (m) (continued)

To display a particular entry, enter its Internet address immediately after the command. For example:

```
snmp manager show 126.5.27.3
```

The router responds as follows:

```
SNMP management station

    SNMP manager            : 126.5.27.3
    Send traps to manager   : yes
    Send syslog messages    : no
    Trap community name     : springe
```

traps (tra)

Command purpose

The `snmp traps` command allows you to specify which events (traps) that occur on the router are reported to the management stations in the router 's Manager table. This command works together with the `snmp manager` command.

Command syntax

The syntax of the `traps` command is as follows:

```
HomeOffice: snmp traps <action>
```

where `<action>` is either `change` or `show`.

Using the command

Changing traps setup

1 To change the traps setup in the router, enter `snmp traps change`.

The router responds as follows:

```
Generic Traps
Cold Start <YES or NO> (Yes) :
```

Generic traps are common to all SNMP devices. They are sent to management stations when the router is powered on.

2 To send generic traps to the management station, enter `yes`; otherwise, enter `no`.

The router responds as follows:

```
Link Down <YES or NO> (No) :
```

3 Enter `yes` if you wish to be informed if a link goes down.

This trap applies to Ethernet and Point-to-Point interfaces only.

The router responds as follows:

```
Link Up <YES or NO> (No) :
```

4 Enter `yes` if you wish to be informed if a link comes up.

This trap applies to Ethernet and Point-to-Point interfaces only.

The router responds as follows:

```
Invalid SNMP Manager Address <YES or NO> (No) :
```

traps (tra) (continued)

This trap is activated when a device uses the wrong SNMP community name to try and talk to the router.

5 Enter `yes` if you wish to capture this trap.

The router responds as follows:

```
Enterprise Traps
   Management Session Started <YES or NO> (No) :
   Management Session Ended <YES or NO> (No) :
```

These traps are specific to Rapport products. They are sent when a management device opens or closes a management session with the router, either locally or remotely using Telnet.

6 Enter `yes` if you wish to capture these traps.

The router responds as follows:

```
Bad password <YES or NO> (No) :
```

This trap is sent when someone tries to open an administration session using the wrong password.

7 Enter `yes` if you wish to capture this trap.

The router responds as follows:

```
Outgoing Call Open <YES or NO> (No) :
Outgoing Call Close <YES or NO> (No) :
Incoming Call Open <YES or NO> (No) :
Incoming Call Close <YES or NO> (No) :
```

These traps report the opening or closing of ISDN calls to the management stations in the router's Manager table.

8 Enter `yes` if you wish to capture these traps.

The router responds as follows:

```
Outgoing Call - Max Duration <YES or NO> (No) :
Incoming Call - Max Duration <YES or NO> (No) :
```

These traps report if the specified upper time limit for an incoming or outgoing ISDN call has been exceeded. (The value at which this trap is triggered is set using the `tune` command in the `network` context.)

9 Enter `yes` if you wish to capture these traps.

The router responds as follows:

```
Bandwidth Usage Limit Exceeded <YES or NO> (No) :
```

traps (tra) (continued)

This trap reports if the specified percentage of day allocated for available ISDN bandwidth to be used is exceeded. (The value at which this trap is triggered is set using the `tune` command in the `network` context.)

10 Enter `yes` if you wish to capture this trap.

The router responds as follows:

```
Resource Allocation Failure <YES or NO> (No) :
```

This trap is sent when the router cannot perform some internal function due to a lack of resource (such as disk/flash space, memory, or streams buffers).

11 Enter `yes` if you wish to capture this trap.

Displaying selected traps

To display the traps set up in the router, enter `snmp traps show`.

The Traps Table showing which traps are activated appears.

The `Enabled` column shows which traps are sent to the LAN. This means that the count for a particular kind of trap may increase even if the trap itself is disabled.

The `Count` shows how often an event has occurred.

SNMP Traps Table

Description	Enabled	Count
Cold Start	Yes	1
Link Down	No	0
Link Up	No	0
Invalid SNMP Manager Address	No	0
Management Session Started	Yes	3
Management Session Ended	Yes	3
Bad password	Yes	1
Outgoing Call Open	No	0
Outgoing Call Close	No	0
Incoming Call Open	No	0
Incoming Call Close	No	0
Outgoing Call - Max Duration	No	0
Incoming Call - Max Duration	No	0
Bandwidth Usage Limit Exceeded	No	0
Resource Allocation Failure	No	0

validate (v)

Command purpose

The `snmp validate` command enables and disables the filtering of incoming SNMP requests, using the Community and Manager tables.

Command syntax

The syntax of the `validate` command is as follows:

```
HomeOffice: snmp validate [show]
```

Using the command

Enabling validation filtering

1 To enable filtering, enter `snmp validate`.

The router responds as follows:

```
Change validation <MANAGER or COMMUNITY> :
```

2 Select the type of validation required.

If you select	Then
`manager`	*the router prompts as follows:* `Validate SNMP requests against managers <ON or OFF> (off):` Respond as required.
`community`	*the router prompts as follows:* `Validate SNMP requests against communities <ON or OFF> (off):` Respond as required.

Displaying the validation setup

To display the current validation setup, enter `snmp validate show`.

```
          Validation of SNMP requests:

    Validate managers    : off
    Validate communities : on
```

System context shell commands

In the `system` context you can use commands to set up various parameters that affect the way your local display works.

In the `system` context, the command prompt is

```
HomeOffice: system
```

The following commands are described in this section:

Command	Shortcut	Description
backup	b	Copies the current configuration.
configuration	conf	Generates a summary of the unit configuration.
edit	e	Alters the command recall facility.
isdn	i	Selects the switch at the telephone company end of your connection.
more	m	Enables or disables the pager `more`.
password	pa	Changes the password for access to privileged commands.
prompt	prom	Defines the privileged level prompt.
protocols	prot	Enables or disables a protocol.
reset	rst	Returns the configuration to factory default values.

—continued—

Command	Shortcut	Description
restore	r	Restores a copy of saved configuration.
save	sa	Saves the router's configuration.
security	se	Encrypts sensitive stored information.
signon	si	Defines the sign-on message.
statistics	ss	Displays buffer and restart statistics.
store	st	Retrieves statistics on the non-volatile memory of your router.
timeout	ti	Specifies the command interface timeout.
trace	tra	Generates debug-like outputs for technical support personnel.
upgrade	upg	Upgrades the unit's software from a TFTP server on the network.
version	v	Displays information about this version of the router.
warnings	w	Shows all the warning messages.

To display a list of available commands, enter `help`. To exit to non-privileged level, enter `quit`.

backup (b)

Command purpose

The `system backup` command allows you to make a copy of the current configuration to a remote TFTP host over the WAN or LAN.

Command syntax

The syntax of the `backup` command is as follows:

```
HomeOffice: system backup
```

Using the command

1 To create a copy of the configuration file, enter `system backup`.

The router prompts as follows:

```
Host <Internet address> :
```

2 Enter the Internet address of the TFTP server to which you are copying the configuration.

The router prompts as follows:

```
Remote file name :
```

3 Enter a remote file name.

This is the name of the file that contains the configuration details of the router.

Any configuration that has changed is saved. A message then indicates that the configuration is being copied:

```
Saving changed configuration.
Copying config to 139.76.45.33:hosave.cfg
.............125K
.............256K
.............354K
.............516K
566864 octets transferred
File copied successfully in 28 seconds
```

configuration (conf)

Command purpose

The `system configuration` command generates a comprehensive summary of the router's configuration.

The summary includes details of interface types and configurations, and circuit information, depending on how your router is set up.

> ***Note:*** This command provides useful information for technical support if you have a problem with the router. The configuration summary is also useful for your own reference.

Command syntax

The syntax of the `configuration` command is as follows:

```
HomeOffice: system configuration
```

Using the command

To display the router's configuration, enter `system configuration`.

To produce a more extensive display that includes dynamic information, enter `system configuration verbose.`

The following example shows a portion of a configuration summary:

```
                  Configuration Summary
                  ---------------------
            ----- Unit wide configuration -----
system version

    Product name      : HomeOffice Router
    Serial number     : NNTM420Y100554
    Software version  : 2.1.1 NT (12 May 1998)
    MC68360 CPU rev   : C
    ISDN variant      : S/T-ISDN
    Time running      :  53m 40s
    Interfaces : eth1      isdn2
    Protocols  : bridge    ip        ipx
    ISDN Software Version:
    SpiderISDN V2.00.01[160], National ISDN 1 (North America))
```

edit (e)

Command purpose

The `system edit` command allows you to alter the command recall facility.

Command syntax

The syntax of the `edit` command is as follows:

```
HomeOffice: system edit
```

Using the command

1 To define the command recall capabilities of the router, enter `system edit`.

The router prompts as follows:

```
Command line editing mode <NONE, FULL or
VT100> (full):
```

2 Do the following:

Option	Description
`none`	With this option, you cannot access previous commands that you have typed.
`full`	This option allows you to use either the arrow keys or control characters to recall commands.
`VT100`	With this option, you can use the arrow keys to see previous command lines, but you cannot use control keys. You should choose this option if you are a Windows95 Telnet user.

isdn (i)

Command purpose

The `system isdn` command lets you configure the router with details about the ISDN service provided by your telephone company.

> ***Note:*** This command is not available if your unit has been factory configured to NTT (Japanese) ISDN.

Release 2.0 introduces the auto-detect feature that determines the type of switch being used by the telephone company. If you choose a North American switch type, auto-switch detection is enabled. You can use the auto-detect detection to show whether you have selected the correct switch type.

Command syntax

The syntax of the `isdn` command is as follows:

```
HomeOffice: system isdn
```

Using the command

1 To determine the type of ISDN switch used by your service provider, enter `system isdn`.

When you press <Enter>, the router displays a prompt similar to the following:

```
ISDN Switch Type <EURO-ISDN, NI-1, NI-2,
ATT-CUSTOM or AUSTEL> (euro-isdn) :
```

2 Select the type of switch that you require. For example `NI-1`.

The following prompt appears:

```
ISDN line power detect <YES or NO> (no) :
```

This prompt allows you to activate or deactivate the power detect option. Power detect determines whether the switch you have selected is on or off by detecting whether the switch is sending power down the line.

isdn (i) (continued)

3 Do the following:

If	Then
you have an S/T interface and are connected to an NT-1	select `NO` or press <Enter>.
you have a U-interface, or you are not using an NT-1	consult your telephone company about the type of S/T interface it is providing to determine the phantom power setting.
your organization is using a PBX	contact your network administrator. The network administrator should consult the PBX manual to see if power detection is supported.
the interface supports power detection	select `YES` at the above prompt.

The changes you have made appear:

```
ISDN global configuration:
ISDN Switch Type : National ISDN 1 (North America)
ISDN line power detect : No
ISDN global configuration updated
```

This change takes effect the next time the unit software is restarted using `top boot`. Restart the unit for these changes to take place.

isdn (i) (continued)

Using auto-detect

To determine if you have selected the correct switch type, you can use auto-detect. The router must be connected to the ISDN line in order for this feature to work. Do the following:

1 Ensure you have selected a North American switch type using the `system isdn` command.

2 Use the `top boot` command to reboot your unit.

The router auto-detects the actual switch type and will use this switch type regardless of the setting you have chosen.

3 Type `system isdn show` and press <Enter>.

This command shows your ISDN switch type setting.

The following appears:

```
ISDN global configuration:
ISDN Switch Type : National ISDN 1 (North America)
(current : whatever the actual switch type is)
ISDN line power detect : No
```

more (m)

Command purpose

The `system more` command lets you specify whether output will be punctuated by `--MORE--` at suitable intervals.

Generally, `MORE` divides screen output into blocks of 24 lines, but some commands, such as `statistics`, use it to page output into smaller logical chunks.

Command syntax

The syntax of the `more` command is as follows:

```
HomeOffice: system more
```

Using the command

1 To instruct the router to display --MORE-- when required, enter `system more`.

The router prompts as follows:

```
Page screen output using more <ON or OFF> (on):
```

2 Do the following:

If	Then
you want the router to display MORE when required	enter `on`. This is the default.
you do not want the router to display MORE, or if the user interface is being driven by a computer application	enter `off`.

password (pa)

Command purpose

The `system password` command changes the password used to enter the administration level.

Command syntax

The syntax of the `password` command is as follows:

```
HomeOffice: system password
```

Using the command

To change the administration password, enter `system password`.

The router prompts for the new password. This password can be up to 20 characters. Since what you type does not appear on screen, the router prompts for the new password a second time, to confirm that you did not type it incorrectly.

If you do not want a password at the administration level, press <Enter> at the new password prompt.

> ***Note:*** When you change the password, take note of it and store it in a safe place. If you forget the password, contact your technical support representative.

prompt (prom)

Command purpose

The `system prompt` command changes the prompt message displayed by the router at the privileged level. The prompt can be any message up to 80 characters long.

Command syntax

The syntax of the `prompt` command is as follows:

```
HomeOffice: system prompt [show]
```

Using the command

Changing the prompt

To change the system prompt, enter `system prompt`.

Entering `none` means there is no prompt.

To include a new line in the prompt, use the characters `\n`.

Press <Enter> to keep the default prompt.

Displaying the prompt

To display the system prompt, enter `system prompt show`.

protocols (prot)

Command purpose

The `system protocols` command enables and disables the protocols running on the router.

> ***Note:*** When your router is delivered, the IP and IPX protocols are already enabled.

Command syntax

The syntax of the `protocols` command is as follows:

```
HomeOffice: system protocols
```

Using the command

Enabling or disabling system protocols

1 To enable or disable the IP or IPX protocols, enter `system protocols`.

The router prompts as follows:.

```
Protocols <IP, IPX, SHOW> :
```

2 Enter the protocol you want to temporarily disable or re-enable.

The router displays a prompt similar to the following:

```
IPX Enabled <YES or NO> (yes) :
```

When you press <Enter>, you see:

```
  Routing Protocol Information

  Protocol Enabled  Routing
    IP     Yes      Yes
    IPX    No       Yes
```

This change takes effect the next time the unit software is restarted using `top boot`.

In this example, IPX is disabled.

protocols (prot) (continued)

The following information appears for each protocol:

- `Enabled`: indicates whether or not you have enabled the protocol
- `Routing`: indicates the current state of the protocol and if packets are being transmitted

Note 1: To activate the enabled protocol and begin routing with it, leave the admin level (`quit` command) and restart the router.

Note 2: Disabled protocols may be bridged on a bridge-only interface or on a bridge-routing interface.

Displaying the protocol status

To display the current protocol status, enter `system protocols show`.

The following appears:

```
Routing Protocol Information

  Protocol Enabled  Routing
    IP     Yes      Yes
    IPX    Yes      Yes
```

reset (rst)

Command purpose

The `system reset` command allows you to remove any configuration you have changed, added, or deleted on your router, and return it to the factory default values.

You may want to use this command because

- you are unsure of the current configuration and want to start again
- you want to move the router to another part of the network or to another site

Command syntax

The syntax of the `reset` command is as follows:

```
HomeOffice: system reset
```

Using the command

1 To start reconfiguring the router from the beginning, enter `system reset`.

When you press <Enter>, you see the following warning:

```
                *** WARNING ***
This will remove all user configuration, and reset
the unit to the factory defaults.
The unit will restart immediately, and take about
15 seconds to boot.
Reset the non-volatile storage <YES or NO> :
```

2 If you wish to continue, select YES.

You are warned not to switch off your router until the reset is complete.

```
************************************************************
DO NOT POWER THE UNIT OFF BEFORE THE SIGN-ON PROMPT REAPPEARS
************************************************************
Resetting non-volatile storage....
```

reset (rst) (continued)

Within 30 seconds, the router informs you that the reset is complete.

```
Resetting non-volatile storage... complete.
Restarting HomeOffice Router .....

Rapport HomeOffice Router
```

You may now begin re-configuring the unit, if necessary.

restore (r)

Command purpose

The `system restore` command allows you to transfer a configuration from a host to a router.

Command syntax

The syntax of the `restore` command is as follows:

```
HomeOffice: system restore
```

Using the command

1 To copy configuration from a host to the router, enter `system restore`.

The router prompts as follows:

```
Host <Internet address> :
```

2 Enter the Internet address or host name of the TFTP server from which you are copying the configuration.

The router prompts as follows:

```
Remote file name : hosave.cfg
```

3 Enter the remote file name.

This is the name of the file on the host that contains the device's saved configuration details.

The router restarts automatically before the new configuration is activated.

save (sa)

Command purpose

The `system save` command lets you save the router's configuration. You should use this command only if you are carrying out a software upgrade.

Command syntax

The syntax of the `save` command is as follows:

```
HomeOffice: system save
```

Using the command

To save the system configuration, enter `system save`.

The router saves the configuration immediately.

security (se)

Command purpose

The `system security` command encrypts sensitive stored information. You can also use this command to encrypt an entire user configuration. This is especially useful for Internet Service Providers that do not want the user to change the configuration of a device.

Command syntax

The syntax of the `security` command is as follows:

```
HomeOffice: system security
```

Using the command

1 To secure the configuration of the router so that it cannot be changed, enter `system security`.

The router prompts as follows:

```
New encryption key <up to 15 characters or NONE> :
```

2 Enter your encryption key and keep it in a secure place.

The router prompts as follows:

```
Encrypt and save current configuration <YES or NO> :
```

3 Enter `no` if you want to decrypt information that was previously encrypted.

signon (si)

Command purpose

The `system signon` command changes the message displayed when you first enter user level or remote administration.

Command syntax

The syntax of the `signon` command is as follows:

```
HomeOffice: system signon
```

Using the command

To change the system sign-on prompt, enter `system signon`.

If you enter `none`, there will be no sign-on message. Press <Enter> to leave the sign-on message unchanged.

The sign-on message can be up to 120 characters long. New lines can be included in the sign-on message by using the characters `\n` for a new line.

statistics (ss)

Command purpose

The `system statistics` command displays buffer, queue, restart, and stream statistics.

> ***Note:*** The `QUEUE`, `MEMORY`, and `STREAM` parameters are normally only used by technical support personnel, and are not documented here.

Command syntax

The syntax of the `statistics` command is as follows:

```
HomeOffice: system statistics [buffer]
```

Using the command

1 To display router statistics, enter `system statistics`.

The router prompts as follows:

```
Statistics <BUFFER, MEMORY, QUEUE, or STREAM> :
```

2 Enter `buffer`.

The number of streams buffers being used, and their sizes appear.

On the router, for example, the display will look similar to the following:

```
                    STREAMS buffers
Size      Maximum     Current        Buffers      Allocation
(bytes)  allocation  allocation      in use         failures
      4        1024          32          10                0
     16        1024          10           4                0
     64        1287          18           8                0
    256         256          19          18                0
    592          64           3           3                0
   1648         128          25          24                0
   2048           4           1           1                0
 driver          50          40          40                0
headers        3000         126         107                0
Unused memory 252092 bytes (lowest 252092 bytes) in 1 fragments
```

store (st)

Command purpose

The `system store` command allows you to retrieve statistics about the non-volatile memory in your router. It also allows you to browse the directory structure on the non-volatile memory.

This command is useful if you experience difficulties and need to provide support engineers with information on the non-volatile memory of your router.

Command syntax

The syntax of the `store` command is as follows:

```
HomeOffice: system store
```

Using the command

1 To retrieve non-volatile memory statistics, enter `system store`.

The router prompts as follows:

```
Storage <STATISTICS or DIRECTORY> (statistics) :
```

2 Do the following:

If	Then

you want to see how much non-volatile memory is used by the system and user configurations	select `statistics`.
	The router displays the statistics including the amount of free space remaining.
	`Storage statistics:`
	`  System  :      524 bytes`
	`  User    :    18304 bytes`
	`  Free    :    42608 bytes`

you want to view information about a particular directory	select `directory`. The router prompts for the directory name. `Directory to show (/) :` Enter the name of the directory you want to view. The router displays a list of all files stored within the non-volatile memory.

timeout (ti)

Command purpose

The `system timeout` command lets you specify the length of the command interface time-out when idle. This time-out applies to all commands and to the privileged mode. When the timer expires, you are returned to non-privileged mode.

Command syntax

The syntax of the `timeout` command is as follows:

```
HomeOffice: system timeout [show]
```

Using the command

Defining the time-out value

1 To define the command interface time-out value, enter `system timeout`.

The router prompts for the following:

```
Command interface timeout in minutes <1-60 or
INFINITY> (2):
```

2 Enter the number of minutes in which the timer should expire or enter `infinity`.

The default is two minutes. If you enter `infinity`, the command interface will never time out.

Displaying the time-out value

To display the current time-out setting, enter `system timeout show`.

The following appears:

```
Command and parameter prompts will time out after 2
minutes.
```

trace (tra)

Command purpose

The `system trace` command switches on and off, various debug-like outputs that are generated during the operation of the router. It is designed for use by technical support personnel.

Command syntax

The syntax of the `timeout` command is as follows:

```
HomeOffice: system trace <action>
```

where <action> is `enabled` to turn system trace on, or `disabled` to turn system trace off.

Using the command

Displaying the internal buffer

To display the internal buffer, enter `system trace`.

The first screen of information appears. To display more information, do one of the following:

- Press <space bar> to display another screen of information.
- Press <Enter> to display another line of information.

Displaying a continuous stream of trace information

To display a continuous stream of information, enter `system trace continuous`.

To stop, press <Ctrl-C>.

Displaying trace information for ISDN layers 2 and 3 traffic

To display ISDN layer 2 and layer 3 traffic on the D-channel (in hexadecimal format), enter `system trace isdn enabled`.

To discontinue, enter `system trace isdn disabled`.

trace (tra) (continued)

Output sample

The following is an example of information captured with the `system trace continuous` command:

```
Continuous Trace information.   Enter <Ctrl C> to
interrupt trace.
3  Image number 51 built at Mon Apr  6 14:43:18 BST
1998
4  H/W: HomeOffice   Bridge/Router
5  S/W: 2.1H D22 (QA regression) (06 Apr 1998)
6  FFS3 verify: 0 bad sectors
7  available_protocols = 0x3
8  enabled_protocols   = 0x3
9  routing_protocols   = 0x303
10  U interface found
11  Install Slots
12  Slot  1: ethernet
13  Slot  2: ISDN BRI
14  DISK restore: system, SNMP, INET, IP, IPX,
bridge, network.
15  Virtual I/F 1 is Disabled in Config.
16  DISK restore: complete.
17  start_isdn: interface 1, usnid 0x42 (B) lsnid
0x42 (B)--> S105/S106 analog ports 0x1
18  ---> INFO TC OUT is set for 0x2
19  ---> INFO TC IN is set for 0x4B
20  TUNING 2 ADDRESSES
21  Vox internal initialization.
22  --> Voice port 1 is fitted
23  --> Voice port 2 is missing
24  WHOA!! Open DIGIVOX
25  DIGIVOX OPEN COMPLETE
26  DVOX OPEN
27  DVOX: Initializing Card struct
28  DEVICE 0
29  DVOX OPEN COMPLETE
30  DVOX IOCTL
31  XE register VC stream with digivox
32  --> Send DVOX_REGISTRATION
33  XE->DIGI: 17
34  REGISTERING 0
35  REGISTER CALL CONTROL DEV 0
36  XE reset RDB daughtercard.
37  --> Send DVOX_RESET
38  XE->DIGI: 22
```

trace (tra) (continued)

```
39  DVOX: Resetting DVox
40  UNBLOCKING ACTIVITY TIMER
41  DVOX: CARD RESET 1
42  down: XN_LISTEN (72F8938 0)
43    up: XN_LISTEN (72F8938 72F8698)
44  +++ LINK PBX circuit
45  ARP   [arp_str.c     :1007] WARN  : IOCTL: cmd
4DE0, error 19
46  SYSTEM RUNNING (tracing is disabled)
47
48  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
49  DVOX: RCVD ACK
50  ACK FOR STATUS_REQUEST
51  DVOX: RCVD STATUS_PASS
52  DVOX: TX  ACK DL 0 : QU 0
53  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
54  DVOX: RCVD ACK
55  ACK FOR STATUS_REQUEST
56  DVOX: RCVD STATUS_PASS
57  DVOX: TX  ACK DL 0 : QU 0
58  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
59  DVOX: RCVD ACK
60  ACK FOR STATUS_REQUEST
61  DVOX: RCVD STATUS_PASS
62  DVOX: TX  ACK DL 0 : QU 0
63  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
64  DVOX: RCVD ACK
65  ACK FOR STATUS_REQUEST
66  DVOX: RCVD STATUS_PASS
67  DVOX: TX  ACK DL 0 : QU 0
68  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
69  DVOX: RCVD ACK
70  ACK FOR STATUS_REQUEST
71  DVOX: RCVD STATUS_PASS
72  DVOX: TX  ACK DL 0 : QU 0
73  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
74  DVOX: RCVD ACK
75  ACK FOR STATUS_REQUEST
76  DVOX: RCVD STATUS_PASS
77  DVOX: TX  ACK DL 0 : QU 0
78  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
79  DVOX: RCVD ACK
80  ACK FOR STATUS_REQUEST
81  DVOX: RCVD STATUS_PASS
82  DVOX: TX  ACK DL 0 : QU 0
```

trace (tra) (continued)

```
 83  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
 84  DVOX: RCVD ACK
 85  ACK FOR STATUS_REQUEST
 86  DVOX: RCVD STATUS_PASS
 87  DVOX: TX  ACK DL 0 : QU 0
 88  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
 89  DVOX: RCVD ACK
 90  ACK FOR STATUS_REQUEST
 91  DVOX: RCVD STATUS_PASS
 92  DVOX: TX  ACK DL 0 : QU 0
 93  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
 94  DVOX: RCVD ACK
 95  ACK FOR STATUS_REQUEST
 96  DVOX: RCVD STATUS_PASS
 97  DVOX: TX  ACK DL 0 : QU 0
 98  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
 99  DVOX: RCVD ACK
100  ACK FOR STATUS_REQUEST
101  DVOX: RCVD STATUS_PASS
102  DVOX: TX  ACK DL 0 : QU 0
103  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
104  DVOX: RCVD ACK
105  ACK FOR STATUS_REQUEST
106  DVOX: RCVD STATUS_PASS
107  DVOX: TX  ACK DL 0 : QU 0
108  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
109  DVOX: RCVD ACK
110  ACK FOR STATUS_REQUEST
111  DVOX: RCVD STATUS_PASS
112  DVOX: TX  ACK DL 0 : QU 0
113  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
114  DVOX: RCVD ACK
115  ACK FOR STATUS_REQUEST
116  DVOX: RCVD STATUS_PASS
117  DVOX: TX  ACK DL 0 : QU 0
118  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
119  DVOX: RCVD ACK
120  ACK FOR STATUS_REQUEST
121  DVOX: RCVD STATUS_PASS
122  DVOX: TX  ACK DL 0 : QU 0
123  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
124  DVOX: RCVD ACK
125  ACK FOR STATUS_REQUEST
126  DVOX: RCVD STATUS_PASS
127  DVOX: TX  ACK DL 0 : QU 0
128  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
```

trace (tra) (continued)

```
129  DVOX: RCVD ACK
130  ACK FOR STATUS_REQUEST
131  DVOX: RCVD STATUS_PASS
132  DVOX: TX  ACK DL 0 : QU 0
133  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
134  DVOX: RCVD ACK
135  ACK FOR STATUS_REQUEST
136  DVOX: RCVD STATUS_PASS
137  DVOX: TX  ACK DL 0 : QU 0
138  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
139  DVOX: RCVD ACK
140  ACK FOR STATUS_REQUEST
141  DVOX: RCVD STATUS_PASS
142  DVOX: TX  ACK DL 0 : QU 0
143  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
144  DVOX: RCVD ACK
145  ACK FOR STATUS_REQUEST
146  DVOX: RCVD STATUS_PASS
147  DVOX: TX  ACK DL 0 : QU 0
148  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
149  DVOX: RCVD ACK
150  ACK FOR STATUS_REQUEST
151  DVOX: RCVD STATUS_PASS
152  DVOX: TX  ACK DL 0 : QU 0
153  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
154  DVOX: RCVD ACK
155  ACK FOR STATUS_REQUEST
156  DVOX: RCVD STATUS_PASS
157  DVOX: TX  ACK DL 0 : QU 0
158  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
159  DVOX: RCVD ACK
160  ACK FOR STATUS_REQUEST
161  DVOX: RCVD STATUS_PASS
162  DVOX: TX  ACK DL 0 : QU 0
163  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
164  DVOX: RCVD ACK
165  ACK FOR STATUS_REQUEST
166  DVOX: RCVD STATUS_PASS
167  DVOX: TX  ACK DL 0 : QU 0
168  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
169  DVOX: RCVD ACK
170  ACK FOR STATUS_REQUEST
171  DVOX: RCVD STATUS_PASS
172  DVOX: TX  ACK DL 0 : QU 0
173  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
174  DVOX: RCVD ACK
```

trace (tra) (continued)

```
175  ACK FOR STATUS_REQUEST
176  DVOX: RCVD STATUS_PASS
177  DVOX: TX  ACK DL 0 : QU 0
178  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
179  DVOX: RCVD ACK
180  ACK FOR STATUS_REQUEST
181  DVOX: RCVD STATUS_PASS
182  DVOX: TX  ACK DL 0 : QU 0
183  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
184  DVOX: RCVD ACK
185  ACK FOR STATUS_REQUEST
186  DVOX: RCVD STATUS_PASS
187  DVOX: TX  ACK DL 0 : QU 0
188  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
189  DVOX: RCVD ACK
190  ACK FOR STATUS_REQUEST
191  DVOX: RCVD STATUS_PASS
192  DVOX: TX  ACK DL 0 : QU 0
193  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
194  DVOX: RCVD ACK
195  ACK FOR STATUS_REQUEST
196  DVOX: RCVD STATUS_PASS
197  DVOX: TX  ACK DL 0 : QU 0
198  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
199  DVOX: RCVD ACK
200  ACK FOR STATUS_REQUEST
201  DVOX: RCVD STATUS_PASS
202  DVOX: TX  ACK DL 0 : QU 0
203  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
204  DVOX: RCVD ACK
205  ACK FOR STATUS_REQUEST
206  DVOX: RCVD STATUS_PASS
207  DVOX: TX  ACK DL 0 : QU 0
208  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
209  DVOX: RCVD ACK
210  ACK FOR STATUS_REQUEST
211  DVOX: RCVD STATUS_PASS
212  DVOX: TX  ACK DL 0 : QU 0
213  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
214  DVOX: RCVD ACK
215  ACK FOR STATUS_REQUEST
216  DVOX: RCVD STATUS_PASS
217  DVOX: TX  ACK DL 0 : QU 0
218  DVOX: RCVD OUT_LOCAL
219  DVOX: TX  ACK DL 0 : QU 0
220  --> Got DVOX_OUTGOING
```

trace (tra) (continued)

```
221  - Look for an idle VC:
222  -- Found one!
223  -- Found one!
224   0  0:23:37 isdn2   Meridian         Call out
handset lifted
225  XN_CONNECT from XE:
226  ... From       2513840
227  ... To         NULL
228  ... Layer 1   0x2
229  ==> PBX (Local)
XE_PSM_IDLE--->XE_PSM_CONNECTING
230  down: XN_CONNECT (72F89F8 0)
231    up: XN_SETUPACK (72F89F8 72F85D8)
232    up: XN_CACTIVE (72F89F8 72F85D8)
233  XN_CACTIVE - accept call on B1
234 ---> Route outgoing PBX call to B1 - 0x40 => 56k.
235  ... TDM route B1 Digivox - REWRITE
236  Assuming ISDN B-Channel B1
237  -> Connect PBX (local) to B1
238  --> Outgoing local call.
239  --> Send DVOX_CON_B
240  XE->DIGI: 6
241  XE->DIGI: CON_B 3
242  BLOCKING ACTIVITY TIMER
243  DVOX: TX  DIALTONE DL 1 : QU 0
244  DVOX: RCVD ACK
245  ACK FOR DIALTONE
246  DVOX: RCVD DIAL_DIGIT
247  --> Got DVOX_DIGIT
248  DVOX: TX  ACK DL 0 : QU 0
249  down: XN_INFO (72F89F8 72F85D8)
250  DVOX: RCVD DIAL_DIGIT
251  --> Got DVOX_DIGIT
252  DVOX: TX  ACK DL 0 : QU 0
253  down: XN_INFO (72F89F8 72F85D8)
254  DVOX: RCVD DIAL_DIGIT
255  --> Got DVOX_DIGIT
256  DVOX: TX  ACK DL 0 : QU 0
257  down: XN_INFO (72F89F8 72F85D8)
258  DVOX: RCVD DIAL_DIGIT
259  --> Got DVOX_DIGIT
260  DVOX: TX  ACK DL 0 : QU 0
261  down: XN_INFO (72F89F8 72F85D8)
262  DVOX: RCVD DIAL_DIGIT
263  --> Got DVOX_DIGIT
264  DVOX: TX  ACK DL 0 : QU 0
```

trace (tra) (continued)

```
265  down: XN_INFO (72F89F8 72F85D8)
266    up: XN_ALERTING (72F89F8 72F85D8)
267  xxx Circuit not voice - do not check for
handsfree alert
268  DVOX: RCVD TERMINATE_CALL
269  TERM STATE 5
270  --> Got DVOX_HANGUP
271  ==> PBX (Local)
XE_PSM_CONNECTING--->XE_PSM_CLOSING
272  DVOX: TX  ACK DL 0 : QU 0
273  UNBLOCKING ACTIVITY TIMER
274  down: XN_DISCONN (72F89F8 72F85D8)
275    up: XN_CONNEND (72F89F8 72F85D8)
276  PBX call closing [CONNEND]
277      ISDN cause: 0x10
278      ISDN diag : 0x0
279  -> Disconnect PBX (local) from B1
280  --> Send DVOX_DIS_B
281  XE->DIGI: 8
282  XE->DIGI: DIS_B
283  UNBLOCKING ACTIVITY TIMER
284  Relinquishing ISDN B-Channel B1
285  BRINGUP 2
286  ... TDM route B1 64kbps Data - REWRITE
287   0  0:23:44 isdn2   Meridian       Call out idle
288  ==> PBX (Local) XE_PSM_CLOSING--->XE_PSM_IDLE
289  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
290  DVOX: RCVD ACK
291  ACK FOR STATUS_REQUEST
292  DVOX: RCVD STATUS_PASS
293  DVOX: TX  ACK DL 0 : QU 0
294  DVOX: RCVD ON_OFF_LINE
295  RECV ON_OFF LINE
296  DVOX: TX  ACK DL 0 : QU 0
297  --> Got DVOX_ON_LINE
298  PBX circuit permanent connection disabled.
299  - Look for an idle VC:
300  -- Found one!
301  -- Found one!
302   0  0:23:47 isdn2   Meridian         Call out
handset lifted
303  XN_CONNECT from XE:
304  ... From       2513840
305  ... To         3311
306  ... Layer 1   0x0
```

trace (tra) (continued)

```
307  ==> PBX (Online)
XE_PSM_IDLE--->XE_PSM_CONNECTING
308  down: XN_CONNECT (72F89F8 0)
309  DVOX: RCVD OUTGOING_CALL
310  RECEIVED RDB_OUTGOING_CALL COMMAND
311  DVOX: TX  ACK DL 0 : QU 0
312  --> Got DVOX_OUTGOING
313  --> Send DVOX_CON_B
314  XE->DIGI: 6
315  XE->DIGI: CON_B 8
316  BLOCKING ACTIVITY TIMER
317  DVOX: TX  OUTGOING_CALL DL 0 : QU 0
318  DVOX: RCVD ACK
319  ACK FOR OUTGOING_CALL
320    up: XN_ALERTING (72F89F8 72F85D8)
321  xxx Circuit not voice - do not check for
handsfree alert
322    up: XN_CONNACK (72F89F8 72F85D8)
323    up: XN_CACTIVE (72F89F8 72F85D8)
324  XN_CACTIVE - accept call on B1
325  ---> Route outgoing PBX call to B1 - 0x40 => 56k.
326  ... TDM route B1 Digivox - REWRITE
327  Assuming ISDN B-Channel B1
328  -> Connect PBX (on-line) to B1
329  --> Outgoing on-line call.
330  ==> PBX (Online)
XE_PSM_CONNECTING--->XE_PSM_ENGAGED
331  --> Send DVOX_CON_B
332  XE->DIGI: 6
333  XE->DIGI: CON_B B
334  No ACTION taken on DVOC_CON_B, in state 11
335  ... PBX online call timer settings
336   0  0:23:48 isdn2   Meridian         Call out
connected
337  DVOX: RCVD TERMINATE_CALL
338  TERM STATE 11
339  --> Got DVOX_HANGUP
340  DVOX: TX  ACK DL 0 : QU 0
341  xxx Hookfault 0x0
342  xe_encap_voice_in msg 1 (OFF-HOOK)
343  V1 LIFT (XE_VSM_IDLE)
344  ... Call Out via 0x72310AC
345  - Look for an idle VC:
346  -- Found one!
347   0  0:23:59 isdn2   Fax              Call out
handset lifted
```

trace (tra) (continued)

```
348  XN_CONNECT from XE:
349  ... From       2513740
350  ... To         NULL
351  ... Layer 1   0x2
352  ==> V1 XE_VSM_IDLE--->XE_VSM_HK_OFF_WAIT
353  down: XN_CONNECT (72F8AB8 0)
354    up: XN_CONNEND (72F8AB8 72F8458)
355   0  0:23:59 isdn2   Fax              Call out
rejected
356   0  0:23:59 isdn2   Fax            Reject cause
100 (Invalid information element contents.)
357  ... TDM route B2 64kbps Data - leave alone
358  V1 CLEAR (XE_VSM_HK_OFF_WAIT)
359  ==> V1 XE_VSM_HK_OFF_WAIT--->XE_VSM_HK_OFF_IDLE
360   0  0:23:59 isdn2   Fax            Call out idle
361  xxx PBX connection idle.
362   0  0:24: 0 isdn2   Meridian         Call out
stop (idle timer)
363  down: XN_DISCONN (72F89F8 72F85D8)
364    up: XN_CONNEND (72F89F8 72F85D8)
365  PBX call closing [CONNEND]
366      ISDN cause: 0x10
367      ISDN diag : 0x0
368  ==> PBX (Online)
XE_PSM_ENGAGED--->XE_PSM_CLOSING
369  --> Send DVOX_HANGUP
370  XE->DIGI: 4
371  DVOX: TX  TERMINATE_CALL DL 0 : QU 0
372  UNBLOCKING ACTIVITY TIMER
373  -> Disconnect PBX (on-line) from B1
374  --> Send DVOX_DIS_B
375  XE->DIGI: 8
376  XE->DIGI: DIS_B
377  UNBLOCKING ACTIVITY TIMER
378  Relinquishing ISDN B-Channel B1
379  BRINGUP 2
380  ... TDM route B1 64kbps Data - REWRITE
381   0  0:24: 0 isdn2   Meridian        Call out idle
382  ==> PBX (Online) XE_PSM_CLOSING--->XE_PSM_IDLE
383  DVOX: RCVD ACK
384  ACK FOR TERMINATE_CALL
385  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
386  DVOX: RCVD ACK
387  ACK FOR STATUS_REQUEST
388  DVOX: RCVD STATUS_PASS
389  DVOX: TX  ACK DL 0 : QU 0
```

trace (tra) (continued)

```
390  xxx Hookfault 0x3
391  xe_encap_voice_in msg 0 (ON-HOOK)
392  V1 REPLACE (XE_VSM_HK_OFF_IDLE)
393  ==> V1 XE_VSM_HK_OFF_IDLE--->XE_VSM_IDLE
394  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
395  DVOX: RCVD ACK
396  ACK FOR STATUS_REQUEST
397  DVOX: RCVD STATUS_PASS
398  DVOX: TX  ACK DL 0 : QU 0
399  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
400  DVOX: RCVD ACK
401  ACK FOR STATUS_REQUEST
402  DVOX: RCVD STATUS_PASS
403  DVOX: TX  ACK DL 0 : QU 0
404  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
405  DVOX: RCVD ACK
406  ACK FOR STATUS_REQUEST
407  DVOX: RCVD STATUS_PASS
408  DVOX: TX  ACK DL 0 : QU 0
409  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
410  DVOX: RCVD ACK
411  ACK FOR STATUS_REQUEST
412  DVOX: RCVD STATUS_PASS
413  DVOX: TX  ACK DL 0 : QU 0
414  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
415  DVOX: RCVD ACK
416  ACK FOR STATUS_REQUEST
417  DVOX: RCVD STATUS_PASS
418  DVOX: TX  ACK DL 0 : QU 0
419  - Look for an idle VC:
420  -- Found one!
421   0  0:24:14 isdn2   IONET           P Call out
attempt
422  XN_CONNECT from XE:
423  ... From       NULL
424  ... To         98774660
425  ... Layer 1   0x0
426  down: XN_CONNECT (72F8AB8 0)
427    up: XN_SETUPACK (72F8AB8 72F85D8)
428  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
429  DVOX: RCVD ACK
430  ACK FOR STATUS_REQUEST
431  DVOX: RCVD STATUS_PASS
432  DVOX: TX  ACK DL 0 : QU 0
433  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
434  DVOX: RCVD ACK
```

trace (tra) (continued)

```
435  ACK FOR STATUS_REQUEST
436  DVOX: RCVD STATUS_PASS
437  DVOX: TX  ACK DL 0 : QU 0
438  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
439    up: XN_CONNACK (72F8AB8 72F85D8)
440  DVOX: RCVD ACK
441  ACK FOR STATUS_REQUEST
442  DVOX: RCVD STATUS_PASS
443  DVOX: TX  ACK DL 0 : QU 0
444    up: XN_CACTIVE (72F8AB8 72F85D8)
445  XN_CACTIVE - accept call on B1
446  ---> Route outgoing data call to B1 - 0x2 => 64k.
447  ... TDM route B1 64kbps Data - leave alone
448   0  0:24:19 isdn2   IONET           P Call out
established (Negotiate PPP)
449  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
450  DVOX: RCVD ACK
451  ACK FOR STATUS_REQUEST
452  DVOX: RCVD STATUS_PASS
453  DVOX: TX  ACK DL 0 : QU 0
454   0  0:24:22 isdn2   IONET           P Call out
data transfer state
455  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
456  DVOX: RCVD ACK
457  ACK FOR STATUS_REQUEST
458  DVOX: RCVD STATUS_PASS
459  DVOX: TX  ACK DL 0 : QU 0
460  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
461  DVOX: RCVD ACK
462  ACK FOR STATUS_REQUEST
463  DVOX: RCVD STATUS_PASS
464  DVOX: TX  ACK DL 0 : QU 0
465  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
466  DVOX: RCVD ACK
467  ACK FOR STATUS_REQUEST
468  DVOX: RCVD STATUS_PASS
469  DVOX: TX  ACK DL 0 : QU 0
470  DVOX: TX  STATUS_REQUEST DL 0 : QU 0
471  DVOX: RCVD ACK
472  ACK FOR STATUS_REQUEST
473  DVOX: RCVD STATUS_PASS
474  DVOX: TX  ACK DL 0 : QU 0
```

upgrade (upg)

Command purpose

The `system upgrade` command allows you to upgrade the router software from a TFTP server on the network.

Command syntax

The syntax of the `upgrade` command is as follows:

```
HomeOffice: system upgrade
```

Using the command

CAUTION
Risk of loss of functionality
The router must not, under any circumstances, be switched off until you receive the message that the upgrade has been successfully completed. If you shut down during upgrade your router will not boot. You can restore operation by upgrading the router from a PC that is connected directly to the Admin port.

1 To download upgrade software for the router from a TFTP server on the network, enter `system upgrade`.

The router prompts as follows:

```
Host <Internet address> :
```

2 Enter the TFTP server's IP address.

The router prompts as follows:

```
Remote file name :
```

upgrade (upg) (continued)

3 Enter the name of the upgrade file.

The file download begins. A message similar to the following appears:

```
Copying 89.0.3.161 <150v600.upg> to image.128k
Copying 89.0.3.161 <150v600.upg> to image.256k
```

After the files are copied, the following message appears:

```
Files copied successfully in... seconds
```

The router restarts automatically.

If your PC or terminal is directly connected to the router's Admin interface, the following message should appear:

```
Verifying upgrade image
```

```
Verified Okay
```

Once the upgrade has been completed, you see the following:

```
Upgrade completed successfully
```

```
Restarting unit
```

If you are remotely connected to the router across the LAN or WAN, your Telnet session will hang. The upgrade takes about 30 seconds. You can check that the upgrade has been successfully completed by re-entering remote Admin and typing `system version`.

The current software version appears.

version (v)

Command purpose

The `system version` command displays information on the software version your router is running.

> ***Note:*** You may need this information if you have to contact your supplier for support information, or if you are ordering an upgrade.

Command syntax

The syntax of the `version` command is as follows:

```
HomeOffice: system version
```

Using the command

Enter `system version`.

You see a display similar to the following:

```
Product name      : HomeOffice Router
Serial number     : NNTM420Y100554
Software version  : 2.1H D24 (12 May 1998)
MC68360 CPU rev   : C
ISDN variant      : S/T-ISDN
Time running      :  53m 40s
Interfaces : eth1      isdn2
Protocols  : bridge    ip        ipx
ISDN Software Version:
SpiderISDN V2.00.01[160], National ISDN 1 (North America)

Meridian:
Software version : 9.1.5
Hardware rev.    : 1.0.0
```

warnings (w)

Command purpose

The system `warnings` command displays all the possible warning messages on the router.

> ***Note:*** Critical and non-critical warnings are described in the "Troubleshooting" chapter of the *Meridian HomeOffice II User Guide* (NTP 555-8321-205).

Command syntax

The syntax of the `warnings` command is as follows:

```
HomeOffice: system warnings
```

Using the command

To display a list of all warnings, enter `system warnings`.

The router lists all the possible warnings with their number. They are presented in two lists: `Critical Warnings` and `Non-Critical Warnings`. Generally, the lower the number, the more serious the warning.

To determine the meaning of a particular warning, enter `system warnings` followed by the warning number. For example, `system warnings 34.`

You see a definition of the warning:

```
Critical warning 34:

Circuit is not routing
```

Index

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Meridian
HomeOffice II
Command Shell User Guide

555-8321-910
Release 2.1 Standard 01.01
July 1998

NORTEL
NORTHERN TELECOM