LRU4240

Dual Trunk E1 Router
User Guide

Software revision 2.3RT

Part 098-04240-18 Rev. 12
October 2003

TECHNICAL: 0118 96 56 000
SALES: 0870 90 10 750
FAX: 0118 96 55 001
ADDRESS: 464 Basingstoke Road, Reading, Berkshire RG2 0BG
WEB: www.blackbox.co.uk

How to Contact Your Local Black Box

Austria:
Black Box gmbh
Tel: 01 256 98 56
Fax: 01 256 98 50-100
Web Site: www.black-box.at

France:
Black Box Catalogue
Tel: 01 45 60 67 00
Fax: 01 45 60 67 47
Web Site: www.blackbox.fr

Deutschland:
Black Box Deutschland
Tel: 0811/5541-0
Fax: 0811/5541-499
Web Site:
www.blackbox-deutschland.com

Switzerland:
Black Box (Schweiz) AG
Tel: 055 451 70 70
Fax: 055 451 70 75
Web Site: www.black-box.ch

Netherlands:
Black Box Datacom BV
Tel: 03032417700
Fax: 0302414746
Web Site: www.blackbox.nl

Norway:
Black Box Norge as.
Tel: +47 55 300 700
Fax: +47 55 300 701
Web Site: www.blackboxnorge.no

U.S.A. :
Black Box Corporation
Tel: 724-746-5500
Fax: 724-746-0746
Web Site: www.blackbox.com

Brazil:
Black Box Do Brasil.
Tel: (011) 5515-4000
Fax: (011) 5515-4002
Web Site: www.blackbox.com.br

Sweden:
Black Box AB
Tel: +46 8 44 55 870
Fax: +46 8 38 04 30
Web Site: www.Blackbox.ab.se

Italy:
Black Box Italia s.p.a.
Tel: 02 27404 280
Fax: 02 27400 219
Web Site: www.blackbox.it

Denmark:
Black Box Denmark
Tel: +45 5663 3010
Fax: +45 5665 0805
Web Site:
Web Site: Web Site: www.blackbox.dk

Spain:
Black Box Comunicaciones S.A.
Tel: 91 659 0191
Fax: 91 623 9784
Web Site: www.blackbox.es

Belgium:
Black Box Communications S.A. N.V.
Tel: 02 725 85 50
Fax: 02 725 92 12
Web Site: www.blackbox.be

Finland:
Black Box Finland Oy.
Tel: +358 (0) 201 888 888
Fax: +358 (0) 201 888 808
Web Site: www.blackbox.fi

Chile:
Black Box Chile
Tel: 00 562 6680 141
Fax: 00 562 6680 140
Web Site: www.Blackbox.cl

Australia:
Black Box Network Services Australia P/L
Tel: 03-9879-7100
Fax: 03-9870-2955
Web Site: www.blackboxoz.com.au

Copyright

ISO Compliance

Products Manufactured Under
An ISO 9001 Certified
Quality Management System

Warning

The Dual Trunk E1 Router complies with FCC Part 15 of the Federal Communications Commission (FCC) Rules concerning radio frequency emissions for Class A computing devices. The following section is required by the FCC.

Caution

In accordance with FCC Part 15 section 15.21, changes or modifications made by the buyer that are not expressly approved by BLACK BOX Ltd could void the buyer's authority to operate this equipment.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This Class A digital device meets all requirementsof the Canadian Interference-Causing Equipment Regulations.
Cet Appareil numerique de la classe A respecte toutes les exigences du Reglement sur le materiel brouilleur du Canada.

NOTE: As per the Voluntary Control Council for Interference by Information Technology Equipment (VCCI), the Dual Trunk E1 Router complies with VCCI Class 1 ITE. This equipment is in the 1st Class category (information equipment to be used in commercial and/or industrial areas) and conforms to the standards set by the Voluntary Control Council for Interference by Information Technology Equipment aimed at preventing radio interference in commercial and/or industrial areas. Consequently, when used in a residential area or in an adjacent area thereto, radio interference may be caused to radios and TV receivers, etc. Read the instructions for correct handling.

この装置は、第一種情報装置（商工業地域において使用されるべき情報装置）で商工業地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会(VCCI)基準に適合しております。
従って、住宅地域またはその隣接した地域で使用すると、ラジオ、テレビジョン受信機等に受信障害を与えることがあります。
取扱説明書に従って正しい取り扱いをして下さい。

Regulatory Information

The equipment complies with the following applicable European Directives 73/23/EEC, 89/336/EEC, 92/31/EEC, 93/68/EEC and 1995/5-EC.

Customer Information

The equipment complies with Part 68 of the FCC Rules. You will find the label located on the bottom of the enclosure. This label contains the FCC Registration Number and Ringer Equivalence Number (REN) for this equipment. You must, upon request, provide this information to your telephone company.

Incidence of harm: If your telephone equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC.

Rights of the telephone company: Your telephone company may make changes in its facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

Malfunction of the equipment: In the event this equipment should fail to operate properly, disconnect the unit from the telephone line. Try using another FCC approved telephone in the same telephone jack. If the trouble does not persist and appears to be with this unit, disconnect the unit from the telephone line and discontinue use of the unit until it is repaired. Please note that the telephone company may ask that you disconnect this equipment from the telephone network until the problem has been corrected or until you're sure that the equipment is not malfunctioning.

Preface

AUDIENCE

This *Dual Trunk E1 Router User's Guide* is intended for network professionals who want instructions for installing and configuring their digital service unit router.

ORGANIZATION

Chapter 1, *"Product Overview,"* provides a description of the features of the Dual Trunk E1 Router, and its placement in a Wide Area Network.

Chapter 2, *"Installation,"* provides a description of the LRU4240, the components you should have received in your shipping carton, and the hardware requirements for setting up the LRU4240 in your network.

Chapter 3, *"Terminal Setup,"* provides instructions on connecting your device to a terminal, logging on to the device; explains how to navigate the terminal screens and configure your device to work with your network.

Chapter 4, *"Access Configuration,"* contains information about configuring the LAN and WAN interfaces, the interface IP addresses, NMS IP addresses, Radius authentication, DHCP, and miscellanous management settings.

Chapter 5, *"Bridging Configuration,"* contains configuration procedures for bridging and VLAN Bridging applications

Chapter 6, *"Routing Configuration,"* contains configuration procedures for static and dynamic routing, and Network Address Translation (NAT)

Chapter 7, *"Firewall Configuration,"* contains configuration procedures for the firewall access list

Chapter 8, *"Diagnostics,"* describes the E1 and in-band tests that can be used to verify the operation of the device and its associated cabling and equipment.

Chapter 9, *"Monitoring and Management,"* describes how to monitor and manage the LRU4240 router. Provides instructions on the option of collecting RMON-2 data.

Chapter 10, *"Alarms,"* describes alarm conditions and alarm configuration parameters.

Chapter 11, *"Troubleshooting,"* provides solutions to specific problems.

Appendix A, *"Specifications,"* provides regulatory compliance information, as well as the electrical, physical, and networking characteristics.

Appendix B, *"Cables and Connector Pin Assignments,"* details connector and pin assignments.

Appendix C, *"Software Upgrade"* software upgrades and download procedures.

Appendix D, *"Menus,"* details software menus command and parameters.

Appendix E, "*Router Command Line Interface Reference*" details the router command line interface commands and parameters

CONVENTIONS

This section describes the conventions used to delineate specific types of information throughout Black Box user guides.

Symbols

Symbols denote text that requires special attention. The information contained alongside a symbol corresponds to one of four levels of severity:

NOTE: Follow guidelines in this, or the previous, paragraph to use the Black Box product more effectively.

CAUTION: Follow guidelines in this, or the previous, paragraph to avoid equipment damage or faulty application.

WARNING: Follow the instructions in this, or the previous, paragraph to avoid personal injury.

ELECTRO-STATIC DISCHARGE — CAUTION: Follow the instructions in this, or the previous, paragraph to avoid the discharge of static electricity, and subsequent damage to the equipment.

Typography

This manual delineates the names of files, commands, and actions by using the fonts and typefaces described in the following table:

Typeface or Symbol	Purpose	Example
`Courier Font AaBbCc123`	The names of commands, files, and directories, as well as on-screen computer output.	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% You have mail.`
`Courier Font, Bold AaBbCc123`	The input you provide, as contrasted with on-screen computer output.	`machine_name%` **`su`**
	Keystrokes that you must provide to use the application.	Press **`Ctrl-L`** to refresh the screen.
Palatino Font, Italic AaBbCc123	Command-line placeholder that you replace with a real name or value.	To delete a file, type **`rm`** *filename*
	Book titles, new words or terms, or words that need to be emphasized.	Refer to Chapter 6 in the *User Guide.* These are called *class* options. You *must* be logged in as root to access this directory.
▼ Zapf Dingbats Font	Symbol that denotes a single-step procedure or task. Procedures requiring more than one task are numbered.	
Palatino Font, Bold Blue, Underscore AaBbCc123	Hyperlinks in the table of contents.When viewing the Portable Document Format (PDF) version of the user guide, you can click on one of these to jump directly to the selected subject matter.	
Palatino Font, Blue AaBbCc123 or AaBbCc123	Hyperlinks throughout general text.	
Helvetica Bold	Denotes actual markings on front or back panels.	Attach the cable to the **TERMINAL** port

BLACK BOX TECHNICAL SUPPORT

If you should experience difficulty with the setup and/or operation of your Black Box equipment, the Black Box Technical Support staff can assist you at any time.

Telephone	**0118 96 56 000**
FAX	**0118 96 55 001**

Internet	**www.blackbox.co.uk**

RETURNING A UNIT

Use the following procedure if you need to return a unit for service or repair,

1. **Contact the Black Box Customer Service Department at 0870 90 10 750, or fax a request to 0118 96 55 001 to obtain an ERN (Equipment Returns Number) number.**
2. **Package the unit carefully and, before sealing the shipping carton, include any information you can provide about the problems you are currently experiencing with the unit.**
3. **Attach an address label to the shipping carton. Be sure to include the ERN number:**

Customer Service Department
Black Box
464 Basingstoke Road
Reading, Berkshire RG2 0BG
ERN # _____

SEND US YOUR COMMENTS

Please let us know if this user guide meets your requirements.
Does the manual answer your questions?
Is the manual thorough?
Is the manual easy to use: can you find the information you need?
Is anything missing from the manual?
What would you like to see in the manual?

Black Box	
FAX	**0118 96 55 001**

All suggestions and comments are appreciated.

Product Overview

PRODUCT OVERVIEW

The Dual Trunk E1 Router is an intelligent network access solution providing connectivity to public and private packet-based networks. Available as a standalone unit it integrates a dual CSU/DSU, routing, and WAN Probe in one single platform.

Figure 1-1 Dual Trunk E1 Router

The Dual Trunk E1 Router supports bridging, static routing, and dynamic routing RIP1, RIP2, and OSPF. The two E1 links can be configured as either two independent PPP or Frame Relay links to different destinations, or a single multilink connection (MLPPP or MLFR FRF.16) to one destination for load balancing and link redundancy application. A firewall permits or denies access based on source and destination IP addresses.

Configuration and troubleshooting is accessible to novice and advanced users with the availability of a menu-based Terminal User Interface and an industry-standard Command Line Interface (CLI). Complete router configuration can be automated remotely by downloading router configuration files.

The Dual Trunk E1 Router is SNMP-manageable, offers menu-driven configuration, includes comprehensive diagnostics, in-band management, and network performance monitoring (RMON1 and RMON2). These tools provide visibility on the usage of the WAN connections.

APPLICATIONS

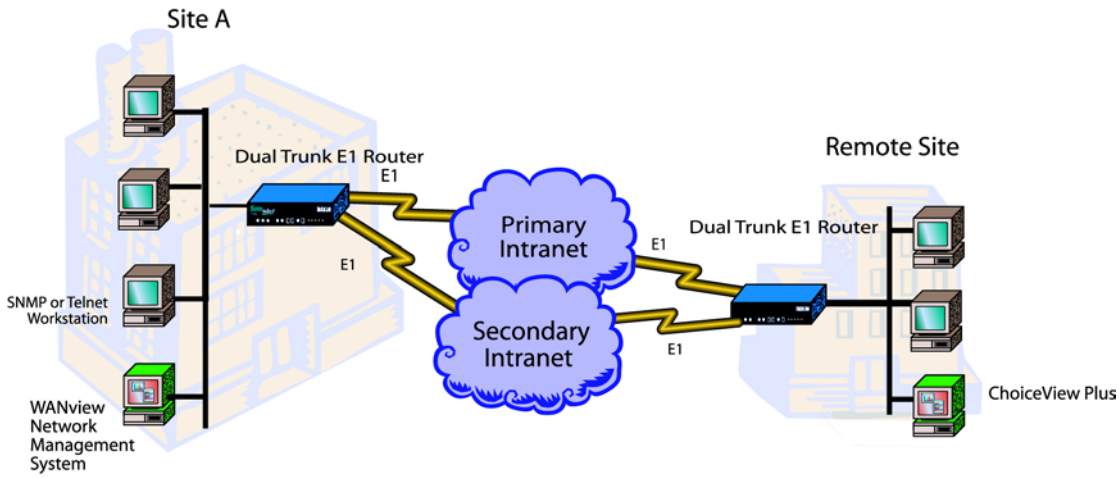
Dual independent links application

Load balancing

When multiple paths exist to the same destination, sending all IP packets on a single route is probably not the most efficient use of the available bandwidth. Load balancing is the practice of distributing traffic among multiple paths to the same destination to achieve higher throughput and avoid delays.

The Dual E1 Trunk Router IP routing engine maintains a cost metric parameter with each route learnt dynamically or programmed statically. If more than one route of equal cost is found for a particular destination, the routing engine will distribute the packets equally among the available routes using a round-robin algorithm.

If multiple routes are found with unequal costs then the route with lesser cost metric is chosen.

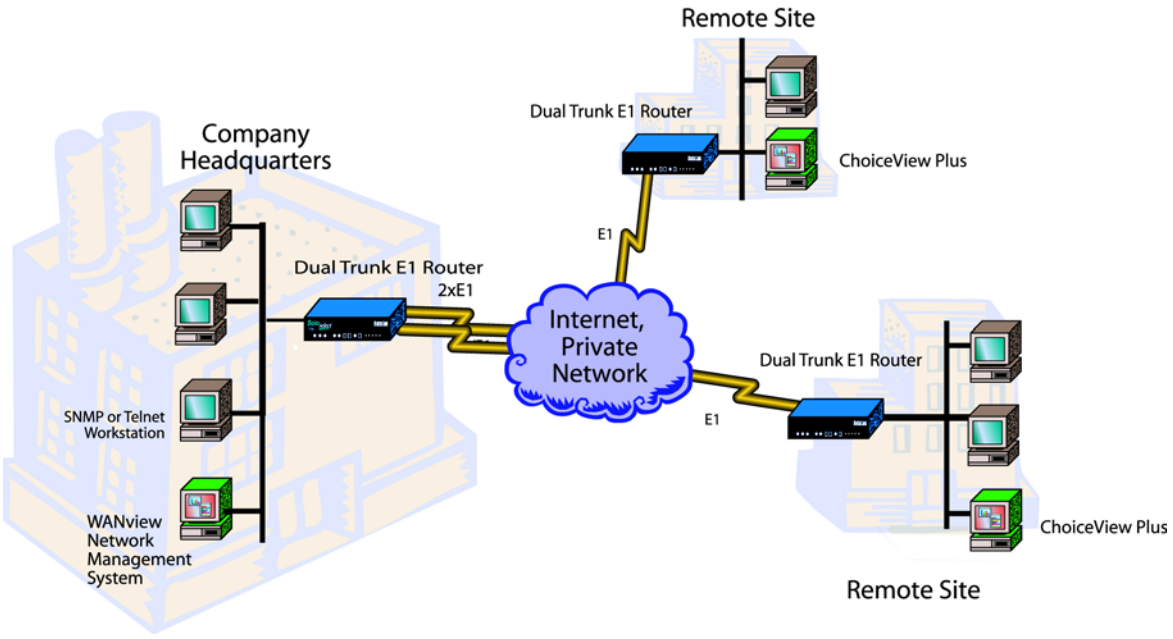


Redundancy

With multiple paths to the same destination, the routing engine also performs redundancy at both the physical layer and the network layer. By monitoring the status of the physical link interface and the PPP negotiation, the unit knows when a link is physically down or a PPP connection is down. When either events occurs, the routing engine will balance traffic to the active link.

Multilink application

Multilink PPP (MLPPP) or Multilink Frame Relay (MLFR) bundles the two E1 ports to pass traffic at twice the speed of a single E1 link. The standard MLPPP per RFC1990 facilitates interoperability with routers from other router vendors.



A pair of Dual E1 Trunk Router can be deployed in a a back-to-back configuration offering a high-speed 4 Mbps point-to-point LAN extension.

Redundancy

With multilink, redundancy is performed at the link layer, if a link is down the traffic is still carried over the active link. If a failed link comes back up again it is automatically added to the bundle, and traffic resumes at twice the speed again.

MONITORING THE ENTIRE WAN PROTOCOL STACK

With the Dual Trunk E1 Router you can monitor the entire WAN protocol stack. Higher level protocols can be monitored using RMON-2. PPP connections can be monitored using RMON-1, and the physical layer can be monitored using diagnostic capabilities as outlined in RFC 1406.

Monitoring Higher Protocol Layers

The Dual Trunk E1 Router includes RMON-2 capabilities. This lets you identify the Top Talkers (256 greatest bandwidth users), and drill down to the Top Applications to see which applications are using the most bandwidth. It also lets you track and report traffic sent between pairs of network addresses and categorizes them by applications and protocols.

Table 1-2 lists the RMON tables supported in RMON-2.

Table 1-1 RMON-2 Tables

RMON-2
Protocol Directory
Network Layer Host
Protocol Distribution
Application Layer Host
Network layer matrix group
Application layer matrix group

Using the optional ChoiceView Plus software application, you can display the statistics gathered by RMON-2.

Table 1-2 RMON Tables

RMON-1 (Provided with Level 2 & 3)	RMON-2 (Option for Level 2 & 3)
History	Protocol Directory
Events	Network Layer Host
Statistics	Protocol Distribution
Alarms	Application Layer Host

To take advantage of the Dual Trunk E1 Router's RMON-2 capabilities, Black Box has created an application, ChoiceView Plus, that allows you to display RMON-2 data in real-time, graphical, and tabular formats.

Installation

Unpacking and Checking Equipment

Before you begin the installation, you need to:

- Unpack and inspect the LRU4240 for damage that may have occurred during shipment
- Save all enclosed packing slips, documents, shipping cartons, and packing materials until you have completed the installation and verified the unit's operation

Package Contents

Make sure that you have received all the items ordered.

- LRU4240 Dual Trunk E1 Router
- A User Guide

Before You Install

Dual Trunk E1 Router operation requires the proper data port, com port and network cables. If you don't have the correct cables, they may be ordered by calling Black Box at (0118) 965-5100 and asking for Inside Sales, or you may order from the Black Box Online Store on our web site: *www.blackbox.co.uk*.

Site Requirements

Install the LRU4240 in accordance with the National Electric Code, ANSI/NFPA 70, Articles 110-16, 110-17, and 110-18. This code defines an access area such as a dedicated equipment room or closet that is clean, well-ventilated, and free of environmental extremes. Allow .5 - 1.0 m (2-3 feet) of clearance around the unit for access during installation.

The operating environment of the LRU4240 is shown in Table .

Table 2-1 Site Environmental Requirements

Item	Specification
Operating Temperature	0°C to 50°C (32°F to 122°F) ambient
Storage Temperature	-20°C to +60°C (-4°F to 140°F)
Relative Humidity	0% to 95% noncondensing
Maximum Altitude	4.6 km (15,000 ft)

Voltages as high as 200 VDC may exist at the telephone company's E1 interface in the form of simplex power. These voltages are hazardous and can cause death or severe injury! Do not proceed with this installation if any voltage is present between the send and receive pairs of the network interface. You can ask the serving telephone company to temporarily disconnect the simplex power during installation.

INSTALLATION

The following procedures outline the steps necessary to install the Dual Trunk E1 Router, power the device, and attach it to a terminal.

Installing the Dual Trunk E1 Router

The Dual Trunk E1 Router should be installed on a flat, stable surface or mounted on a tray.

To install the Dual Trunk E1 Router on a flat surface:

1. **Remove the covering from the four stick-on rubber pads and attach them to the bottom of the unit.**
2. **Place the unit on a flat, stable surface.**

   You may stack other units on top of the Dual Trunk E1 Router.

Installation Using AC Power

To install the Dual Trunk E1 Router using AC power, follow the step below and refer to Figure 2-1:

Insert the power cable into the power receptacle on the Dual Trunk E1 Router rear panel. Connect the other end to the AC outlet.

The LEDs on the front panel flash and status messages appear on the alphanumeric display as the Dual Trunk E1 Router runs the Self Test at power up.

NOTE: DC Power may be used as a primary power source or as a backup power source, should AC power fail.

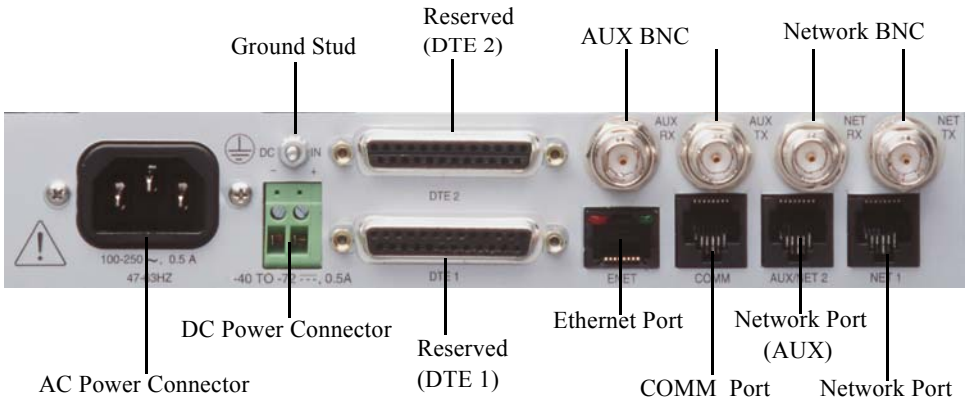


Figure 2-1 Back Panel View–Ports and Ground Stud

Installation Using DC Power

You need a tray cable that is UL recognized 14 AWG, 3 conductors, copper strand wire, electrical power and control cable, type TC: tray cable, 600 V 90°C. Alpha Wire Company No. 45443 is an example.

To connect the Dual Trunk E1 Router to DC power:

1. **Place the unit on a flat surface or tray.**
2. **Make sure the DC power source is off.**
3. **Before you connect the unit to the centralized DC power source, strip 2 inches of jacket material off the tray cable and 1/2 inch of insulation off each wire.**
4. **Connect the -48 V wire to the positive (+) terminal using a small flat screwdriver to fasten the wire.**
5. **Connect the ground wire to the negative (-) terminal using the same method.**

   The unit is designed to operate with negative voltage; therefore, the positive terminal is connected to ground.
6. **Connect a properly grounded third wire to the ground stud near the terminal block using a 1/4 inch wrench and fastening torque of 5 inch-pounds.**
7. **To minimize disturbance to the wires through casual contact, secure the tray cable near the rack frame using multiple cable ties.**

   Use at least four cable ties, a minimum of 4 inches apart. The first tie should be within 6 inches of the terminal block.
8. **Connect the Dual Trunk E1 Router to a DC power source. Turn on power source.**

The LEDs on the front panel flash and status messages appear on the alphanumeric display as the Dual Trunk E1 Router runs the Self Test at power up.

Dual Trunk E1 Router

Terminal Setup

The Dual Trunk E1 Router can be operated using basic front panel controls, or through a more in-depth terminal interface. It is divided into two main sections listed below:

- Navigating the Front Panel
- Terminal Mode

NAVIGATING THE FRONT PANEL

From the front panel, you can:

- View and change configuration parameters
- Run diagnostic tests
- Monitor the Dual Trunk E1 Router status

The front panel allows access to most of the configuration and monitoring features of the Dual Trunk E1 Router. You may find that for regular daily use, the front panel provides a quick and easy means of monitoring the status of your device and changing configuration parameters.

The front panel is controlled using the front panel buttons: EXIT, UP arrow, DOWN arrow, and ENTER. For an explanation of each button's function, see Table 3-1.

Table 3-1 Button Usage

Button	Function
Back/Exit Button	Cancel an option or exit a menu
Up/Back Button	Move backward through the options
Down/Forward Button	Move forward through the options
Enter Button	Select an option

The front panel and its buttons and LEDs are shown on page page 24. If you wish to disable these buttons, enable Protect Mode on Menu-4, Main Configuration using the terminal user interface. You will still be able to view the unit's settings using the buttons, but you will not be able to change the settings.

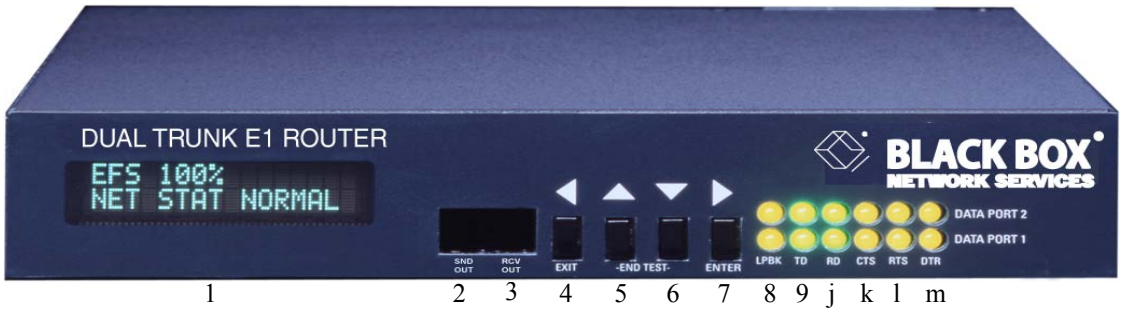


Figure 3-1 Dual Trunk E1 Router Indications and Buttons

#	Description	#	Description
1	Alphanumeric Display	8	Loopback LEDs
2	Reserved	9	Reserved
3	Reserved	j	Reserved
4	Back/Exit Button	k	Reserved
5	Up/Back Button	l	Reserved
6	Down/Forward Button	m	Reserved
7	Enter Button		

The LEDs for the Ethernet port are located in the back of the unit.

Front Panel Display

The front panel alphanumeric display provides a 2-line, 16-character message. It provides access to the Dual Trunk E1 Router via the front panel buttons. Press the UP ARROW and the DOWN ARROW keys to move among the various menus. Using the UP ARROW and DOWN ARROW keys will move you among the categories listed in Table 3-2.

Table 3-2 Front Panel Categories

Field	Function
EFS <XXX>%	The percentage of time the E1 link has run without error.
CONFIGURATION	Access the Dual Trunk E1 Router's basic configuration options, the unit's serial number, and the current software version.
TEST	Run various diagnostics tests.
MONITOR	Track errors and system status parameters.

Default Display

```
EFS <XXX>%
ALL LINKS
NORMAL
```

The EFS Field

To reach the EFS (Error Free Seconds) statistic, press the EXIT Button repeatedly until the EFS category appears on the display. The EFS field presents the percentage of seconds in which no error occurred. The higher the percentage, the more stable the E1 connection.

Error-free seconds are calculated using the following formula:

$$EFS = \frac{GoodSeconds}{TotalSeconds}$$

$$GoodSeconds = AllSeconds - (BadSeconds + UnavailableSeconds)$$

The Configuration Options

To reach the `Configuration` options:

1. **Starting from the default display, press the UP or DOWN Arrow button to move among the fields until the `CONFIGURATION` category appears on the display.**
2. **Press the ENTER button to enter Configuration mode.**

   `UNIT CONFIG` appears on the display.
3. **Press either the UP Arrow or the DOWN Arrow to move through the configuration options. The configuration options are presented in Table 3-3.To select a Configuration option, press the ENTER button.**

   The display changes to reflect the first in the list of editable fields.
4. **Press the UP Arrow or the DOWN Arrow to move through the options in the `CONFIGURATION` menu until the feature you want to change is displayed.**

5. **Press the ENTER button to enter edit mode for the selected feature.**
6. **Use the UP Arrow and/or DOWN Arrow to change the field.**
7. **Press the ENTER button to enter your change.**
8. **Press the EXIT button to leave edit mode.**

Dual Trunk E1 Router Configuration Option

The following table lists the configuration options.

Table 3-3 Dual Trunk E1 Router Configuration Options

Option	Definition

UNIT CONFIG	Allows you to change the UNIT ID, the Date and Time, and the COMM Port Configuration. The options allow you to change:
	• Unit ID
	• Date and Time
	• COMM Port Configuration
	  • Baud Rate
	  • Parity Bits
	  • Word Length
	  • Stop Bits
	  • Xoff/Xon
	• Test Length
	In addition, the UNIT CONFIG option displays the hardware revision, the software revision, and the serial number.

IP CONFIG	Allows you to view of configure your device for use within an IP network. • View the IP address of the COMM port (COMM IP ADD). • View the IP address of the NET port (NET IP ADDRESS). • Configure the IP address for the Ethernet port (ETHERNET IP AD. • Configure the IP mask (ETH IP MASK)

The Test Options

Tests can be run on the WAN ports. To conduct a test from the front panel:

1. **Press the UP Arrow button to move among the fields until the `Test` field appears on the display.**
2. **Press the ENTER button to enter test mode.**

   `SELF TEST` appears on the display.
3. **Press either the UP Arrow or the DOWN Arrow to move through the test options until the desired test is displayed. The following tests are available:**
   - SELF TEST
   - LOOP NET

- LOOP PAYLOAD
- LOOPUP REMOTE
- TEST PATTERN
- LOOPDOWN REMOTE
- LAMP TEST

4. **Press ENTER To select the test. Press ENTER again to run the test.**

   Follow the display prompts to complete the test.

To Stop a Test

If you want to stop a running test, simultaneously press both the DOWN ARROW key and the UP ARROW key on your front panel.

The Monitor Options

The `Monitor` category provides a means of quickly monitoring the status of your network from the alphanumeric display. While many of the `Monitor` options are read only, counters can be cleared and reset to zero.

To reach the `Monitor` options:

1. **Press the UP Arrow button to move among the categories until the `Monitor` category appears on the display.**
2. **Press the ENTER button to enter Monitor mode.**

   `UNIT STATUS` appears on the display.

3. **Press either the UP or DOWN Arrow to move through the monitoring options. The `Monitor` options are in Table 3-4.**

Table 3-4 Monitor Options

Monitor Option	Write Access
UNIT STATUS	Provides timing status. Read only.
NET STATUS	Loss of Signal (LOS), Loss of Frame (LOF), NORMAL. Read only.
PPP STATUS	Provide status of the PPP link.
MLPPP STATUS	Provide status of the Multilink PPP link.
ETHERNET STATUS	Provide status of the Ethernet interface.

TERMINAL USER INTERFACE MODE

The front panel display provides miminal setup, configuration and verification menus. To fully configure your LRU4240 router you will need to access the Terminal User Interface (TUI) directly through the COMM port, or Telnet via the Ethernet port or the WAN ports.

Terminal Interface Navigation

The terminal interface contains a number of menus which are used to configure, monitor, and manage the Dual Trunk E1 Router.

- To navigate the fields in the menus, use the arrow keys on your keypad.
- To select a menu, press the menu number as indicated at the bottom of the menu screen.
- To change a parameter, use the arrow keys to cycle through the available options and press **`Return`** to select the highlighted option.

Setting a Menu Parameter

Use the following procedure to select a parameter, set it, and confirm your action:

NOTE: You can also use the **`u`** (up), **`d`** (down), **`r`** (right), and **`l`** (left) keys in place of the arrow keys.

1. **Move the cursor to a field using the arrow keys, and press `Return` to activate edit mode.**

To change a parameter, use the arrow keys to cycle through the available options and press `Return` to select the highlighted option. In other fields, you will be prompted for the required value. Enter the value, and press `Return`.

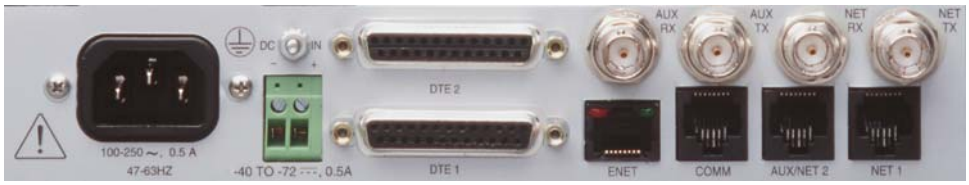
- Attaching the Dual Trunk E1 Router to your terminal
- Using Hyperterm to log on to the Dual Trunk E1 Router
- Configuring access rights

ATTACHING TO A TERMINAL

The Dual Trunk E1 Router can be attached via the COMM Port to the serial port of a server, computer, or terminal. You may need to attach your Dual Trunk E1 Router using the COMM Port on the rear of the device.

▼ **Connect an RJ-45 to DE-9 COMM Port cable from the COMM Port on the Dual Trunk E1 Router to the COMM Port on your terminal.**

To communicate from an ASCII terminal to your device, use the COMM Port connector on the back panel of your Dual Trunk E1 Router (Figure 3-2).



COMM Port

Figure 3-2 COMM Port on Dual Trunk E1 Router

Using the Ethernet port as management interface

As an alternative to managing the Dual Trunk E1 Router via the COMM port, you can manage it directly using the Ethernet port (ENET). You can then Telnet into the device from any workstation in the network. This provides for both local and remote access.

Using Terminal Software

Once you have attached the Dual Trunk E1 Router to a terminal using one of the methods described above, you will need to use terminal emulation software to communicate with, and configure the device. You may use Hyperterm Windows, or the terminal emulation software of your choice. If using Hyperterm, follow the instructions outlined below to set up and run the program.

Terminal Setup

The COMM Port factory default settings on your device are defined as:

- Baud Rate — 38400
- Parity Bit — none
- Word Length — 8
- Stop Bits — 2

Make sure that your terminal software is set to work with these parameters, or use the front panel to alter the default settings. Once you are logged in, the unit's COMM port settings may be changed as shown in the section "Adjusting COMM Port Settings" on page 31. In addition, the following parameters should be set:

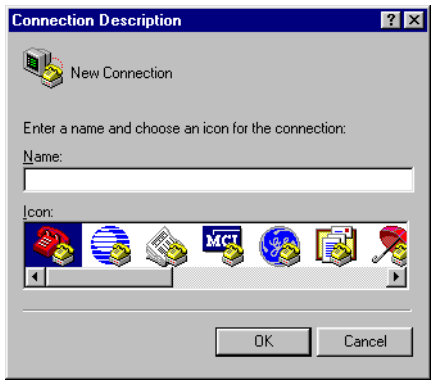
- Hardware Flow Control—none
- Terminal Emulation—VT-100

Hyperterm Windows Setup

Hypterterm is a Windows terminal emulation program that can be used to log on to the unit.

1. **Run Hypertrm.exe.**

2. **Type a `File Name`, choose an icon then click `OK`.**

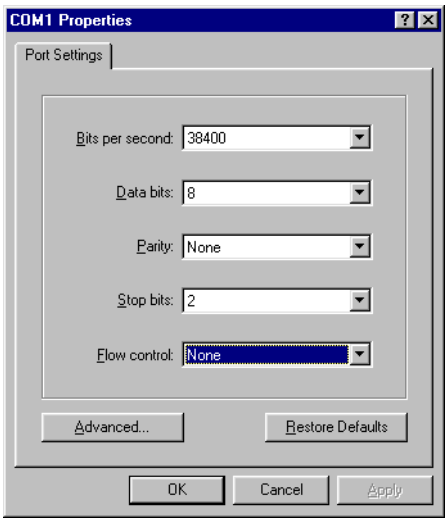


The name allows you to save the settings for future sessions and the icon represent the connection. You can put the icon on your desktop for easy access.

The Connect To properties tab appears (Windows 98) or the Phone Number window appears (Windows 95)

3. **From the `Connect Using` field drop-down list, select `Direct to COM1` (or preferred COM port) then click `OK`. COM1 will be used for the rest of this procedure.**

The COM1 Properties box appears for `Port Settings`.

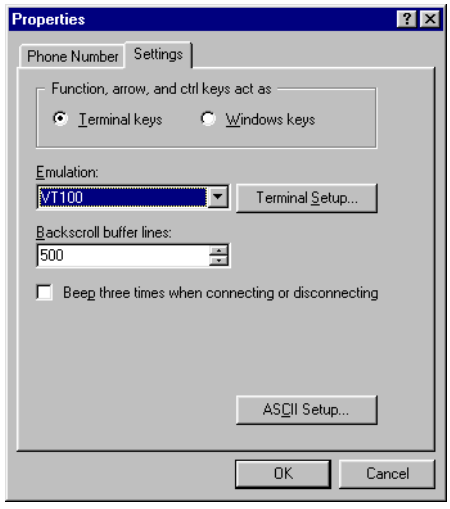


4. **Configure the settings for the COM1 Properties dialog box as shown below:**
   - Data bits per second — 38,400
   - Data bits — 8
   - Parity — None
   - Stop bits — 2
   - Flow control — None

   After configuring the settings, click **OK**

   A blank screen with the cursor blinking appears.

5. **Go to the File pull-down and select Properties. At the properties Dialog box, Click the** `Settings` **tab.**



6. **Set the following:**

a. **`Emulation` field to at VT-100**

b. **`Backscroll buffer lines` to 500.**

Press `Ok`. You can now log on to the Dual Trunk E1 Router**.**

Logging On from a Terminal

To log on to the unit, you must first obtain the unit ID of the device. The unit ID is printed on a small sticker on the back or bottom of the device. You can also retrieve the unit ID via the UNIT CONFIG option of the front panel. For information on using the front panel, see "Navigating The Front Panel" on page 21.

New units have no password assigned. If you are logging in for the first time, you will not need to enter a password. Press return at the prompt and Menu 1, Main Status will appear. Systems with blank IDs are always logged on and cannot be logged off until a unit ID is assigned. For information on assigning an ID, refer to "Setting ID, Date, Time, and Network Timing" on page 34.

The default ID is always a 6-character alphanumeric string that identifies the unit.

If you wish to display or verify the unit ID, press **`Ctrl-x`** five times to display all devices connected to the terminal.

To log on to the Dual Trunk E1 Router:

1. **Press `Ctrl-x`, type the unit ID, and press `Return`.**

   If password is enabled, the system prompts for a password.

   ```
   Now you need a password to log on:
   ```

2. **Type the Superuser or normal user password and press `Return`**

   (For more information on normal and Superuser rights, see "Configuring Access Rights" on page 32).

   Menu-1, Main Status, appears.

   If this menu does not appear, you may have an incorrect ID, a faulty connection on the COMM Port, or an incorrect COMM Port configuration.

3. **Refer to Table 3-5 for Dual Trunk E1 Router messages during logon.**

Table 3-5 Login Prompts

System Messages	Action	Condition
The Terminal User Interface is already in use	Please enter the Superuser password to force the other user to log off or press **`Ctrl-x`** and try again later.	Normal user logged on via Telnet.
Superuser is already logged into the Terminal User Interface. Try again later.	Press **`Ctrl-x`** and try again later.	Superuser logged on.

NOTE: When accessing the unit via Telnet, the system forces you off after the fifth unsuccessful attempt to log on.

Logging Off from a Terminal

To log off, press **`Ctrl-x`**.

The terminal stops responding to your keystrokes when you are logged off.

Adjusting COMM Port Settings

COMM port settings can be modified in the Dual Trunk E1 Router using Menu 8F - COMM Port Configuration.

NOTE: It is possible to disrupt your terminal connection by changing these settings.

The configurable settings are:

- Baud Rate
- Parity
- Word Length
- Stop bits
- Flow control
- DCD

For more information on Menu 8F and available options, see the *4200 WAN Access Platform TUI Reference Guide*.

Logging on from a Telnet Connection

To log on from a Telnet connection, use a terminal or terminal emulation program to access the unit directly.

To log on to the unit user interface using a Telnet connection:

1. **Enter the Telnet COMMand and the Dual Trunk E1 Router IP address.**
   Example of system response: MULTI is unit ID

   ```
   Current ID is MULTI
   MULTI password:
   ```

   If you do not have an ID, you may still log in. A `"Sorry" or Logged Out"` Message will appear. Press **`Ctrl-x`** to bring up a menu. **`Ctrl-x`** will not log you out until an ID is assigned.

2. **Enter the Normal User or Super User password.**

   If you do not have a password, you may still connect. When connected, Menu 1 will appear.

NOTE: If your Dual Trunk E1 Router is set for dial-up mode, that is, using a modem and directly dialing through a standard telephone connection, it is recommended that you DO NOT use a Telnet session to access the unit.

CONFIGURING ACCESS RIGHTS

You can create two access levels to the Dual Trunk E1 Router terminal interface—Superuser access rights and normal user access rights—by entering unique Superuser and normal user passwords in Menu 8C - Miscellaneous Management Configuration.

Assigning User Passwords

Since two access methods are available (using a terminal connected to the COMM Port or a Telnet connection from a remote terminal), you should exercise caution when assigning passwords.

A “no passwords” situation gives any user logging on Superuser access rights. If this user sets only one password, both passwords become the same.

When both passwords are the same, any user logging on with either password gains Superuser rights. As Superuser, the individual has exclusive control of the terminal interface.

NOTE: You must set both passwords to prevent the above situations. Specify unique Superuser and Normal User passwords in Menu-8C.

Access Configuration

Overview of Access Configuration

This chapter contains information about configuring the LAN and WAN interfaces, the interface IP addresses, NMS IP addresses, Radius authentication, DHCP, and miscellanous management settings

Table 4-1 Access configuration procedures

Procedure	Description	Menu	Reference
Configuring LAN interface	To set or modify the Ethernet data port IP address and subnet mask, and the ethernet speed (10MB/Half or 10MB/Full).	Menu-0A Menu-0C	page 35
Setting Unit ID, Date, Time, and E1 Network	To configure the network E1 timing, framing, and coding.	Menu-4A Menu-4B	page 35
Allocating Timeslot for data and voice	To allocate and map fractional dual E1 bandwidth to the Ethernet data port	Menu-6Z	page 37
Configuring WAN protocol	To configure the WAN protocol to: • Single link PPP interface • Dual independent PPP link interfaces • Multilink PPP (MLPPP) interface • Single link Frame Relay interface • Dual links Frame Relay interfaces • Multilink Frame Relay (MFR) interface	Menu-0A	page 38
Configuring Frame Relay DLCIs	To configure statically the DLCI numbers with associated interface.	Menu-0E	page 40
Configuring Link Management Information	To enable or disable LMI, and configure LMI settings, unit location UNIT-U or UNI-N	Menu-0F	page 40
Mapping DLCIs to IP addresses	To configure the mapping of DLCI to the next hop IP addresses statically and manually.	Menu-$IA	page 41
Configuring SLIP	To configure SLIP (Serial Line Interface Protocol) to allow telnet access through the COMM port.	Menu-0A	page 41
Configuring Access Rights	To set the TUI normal and superuser access levels.	Menu-8C	page 42
Configuring Radius Authentication	To configure Radius authentication, user login and password, preventing unauthorized access and changes to the access router TUI.	Menu-8G	page 42
Enabling/Disabling Traffic Monitoring (Optional)	To enable or disable the router from collecting and reporting RMON-1, and RMON-2 statistics. To enable or disable Frame Relay SLA and configure Frame Relay SLA statistics. By default Traffic monitoring is disabled.	Menu-0A Menu-0H	page 44

Table 4-1 Access configuration procedures

Procedure	Description	Menu	Reference
Configuring SNMP	To configure SNMP “get”, “set, and” trap community” strings to prevent unauthorized SNMP management stations from gaining access to the router. Configure up to three Network Management Station (NMS) IP addresses that will receive SNMP trap to report alarms.	Menu-0B	page 44
Configuring Time and Date synchronization	To configure RFC868 compliant time and date synchronization client.	Menu-4T	page 45
Configuring DHCP relay agent	To configure DHCP server IP address and enable DHCP relay agent.	Menu-$K	page 46

CONFIGURING LAN INTERFACE

Table 4-2 Configuring LAN interface

Procedure	Steps
Setting Ethernet port speed	To configure the ethernet speed to 10MB/Half or 10MB/Full. 1.Select Menu-0C 2.Select Data/Speed Mode 3.Select 10MB/Half or 10MB/Full setting. The default value is 10MB/Half.
Modifying Ethernet port IP address	1.Select Menu-0A 2.Select ENET IP Address/Len field 3.Enter the assigned Ethernet port IP Address and the subnet mask

SETTING ID, DATE, TIME, AND NETWORK TIMING

Unit Configuration– Menu 4A

Figure 4-1 shows **Menu 4A Unit Configuration**. The numbers in circles correspond to the procedures for setting the parameters in each field.

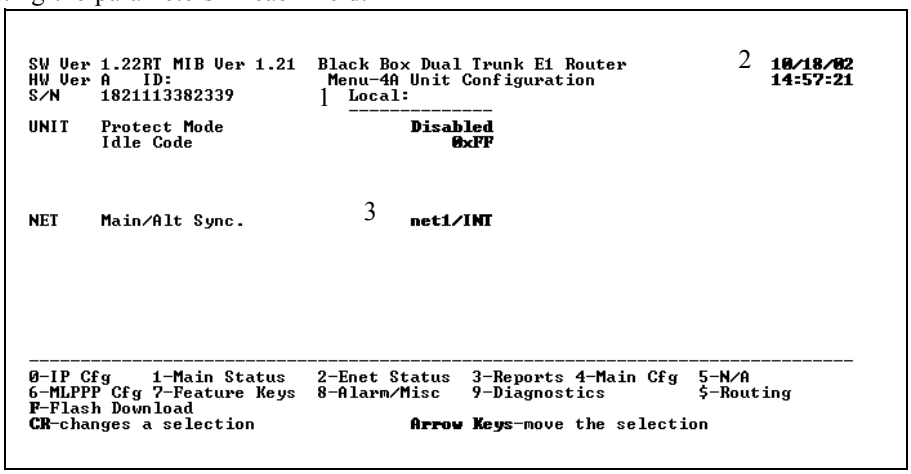


Figure 4-1Menu 4A, Unit Configuration

Table 4-3 Menu-4A- Unit Configuration

Parameter	Description
UNIT ID	**Field** `Local` 1 **(Alphanumeric field identifier at the top of the menu)** The Dual Trunk E1 Router comes factory configured with a unique unit ID. Each Dual Trunk E1 router in your network must have a unique Unit ID. You may use the preconfigured Unit ID or change it to a combination of 6 alpha and numeric characters, but the first character must be an alpha character.

Parameter	Description
DATE	`Date` **or** `time` 2 To change date or time field, select the date or time field at the top of the screen by moving the cursor. Enter date and time as indicated by the prompt at the bottom of the screen. Example: **`2/22/97`** yields `02/22/97` and **`22:4:6`** yields `22:04:06` (The clock is a 24-hour clock.)
UNIT	**Protect Mode** - Enabled or Disabled (default); Enabled - Protect mode prevents you from running tests from the front panel.
NETWORK TIMING	**Main/Alt Sync -** INT, NET1, NET2 Select the timing source for Main and for Alt Sync. The options INT, NET1, or NET2 for Main and Alt Sync. **NET1 or NET2**: Select this option if the network is the clock source. **INT:** Select this option if timing is derived from the internal oscillator in the unit.

Net Configuration and Status

Table 4-4 Menu-4B- Net configuration and status

Parameter	Description
Status	Displays the network status.
Framing	Selects the network framing format from the following options: CRC4 enabled (the default), CRC4 disabled, and unstructured

CONFIGURING TIMESLOT ALLOCATIONS

Timeslot allocation menu is available for single and independent links applications, it is not available with multilink. The timeslot allocation menu-6Z lets you allocate fractional E1 bandwidth and map it to the Ethernet data port. With dual independent links the same selected timeslots will apply to both E1 links.

Table 4-5 Menu-6Z, Timeslot configuration

Parameter	Description
Allocation type	Select the desired timeslot allocation method as Contiguous, Alternate, or Manual. **Contiguous:** To select a range of contiguous timeslots. Contiguous timeslots are always adjacent to each other and in numerical order. To configure contiguous timeslots, specify a valid range of timeslots. such as 17 to 25. **Manual:** Move to a timeslot one at a time, and assign a Data Port to it. This method allows any arbitrary timeslot allocation.
Allocation type	Select
Allocate by port (IDLE, FRAC01 or AUX)	Allocate the selected timeslots for data, or set them to idle. Press the space bar then enter to select: IDLE or FRAC01. **IDLE -** Selected timeslotes will be disabled. **FRAC01 -** Ethernet port
Allocate by port starting and ending timeslots	TS01: Type in the starting timeslot TS31: Type in the ending timeslot.

If you configure timeslots in such a way that contradicts the definition of contiguous, the Dual Trunk E1 Router will automatically set the contradicting timeslots to `Idle`

Table 4-6 Timeslot allocation procedures

Procedure	Steps
Allocating contiguous timeslots to data services	1.Set allocation type to Contiguous 2.Select FRAC01 port for Ethernet port in Allocate by Port 3.Enter starting timeslot provided by your carrier 4.Enter ending timeslot provided by your carrier

Table 4-6 Timeslot allocation procedures

Procedure	Steps
Disabling timeslots	Example: setting timelost 1 through 8 to Idle 1.Set allocation type to Contiguous 2.Select Idle in Allocate by Port 3.Enter starting Idle timeslot 4.Enter ending Idle timeslot
Allocating alternate timeslots	Example: timeslot 7 through 17 for data 1.Set allocation type to Alternate 2.Select FRAC01 in Allocate by Port 3.Enter 7 in starting timeslot 4.Enter 17 for end timelot FRAC01 TS07 TS17 384 Kb/S appears in the Allocate by port fiel and timeslots 7, 9, 11, 13, 15, and 17 are allocated to Ethernet port, while all other timeslots are set automatically to idle.
Allocating timeslots manually	To manually allocate timeslots, move to the timeslot and specify the port. You must the other timeslots to Idle. Example: setting timeslots 3,7,9,14, and 15 to Ethernet port. 1.Set allocation type to Manual 2.Select timeslot 1 and set it to Idle 3.Repeat step 2 to configure the other timeslots to Idle

CONFIGURING WAN PROTOCOL

The WAN protocol can be configured to Frame Relay, Multilink Frame Relay, PPP, or MLPPP.

Configuring Single Link PPP Interface

Table 4-7 Single PPP Link Configuration

Procedure	Steps
Set router traffic type to PPP	1.Set Menu-0A- Traffic type field to PPP. 2.Set Menu-0A Multilink Protocol field to No. This disable multilink operation
Set WAN port 1 IP address	1.Set Menu-0A NET IP address and subnet mask

Notice the menus will be configured for PPP operations. The bottom menu will display “6-PPP Cfg”.

Configuring independent PPP links Interfaces

The PPP connection over the first T1/E1 port is assigned the interface port NET1. The second T1/E1 port is assigned the interface port NET2.

Procedure	Purpose
Set router traffic type to PPP	1.Set Menu-0A- Traffic type field to PPP. 2.Set Menu-0A Multilink Protocol field to No.
Set WAN port 1 IP address	1.Set Menu-0A NET1 IP address and subnet mask Assign an IP address and subnet mask to the second T1/E1 link. This will be identified as NET1 link in all the menus.
Set WAN port 2 IP address	1.Set Menu-0A NET2 IP address and subnet mask Assign an IP address and subnet mask to the second T1/E1 link. This will be identified as NET2 link in all the menus

Configuring MLPPP Interface

Procedure	Purpose
Set router traffic type to MLPPP	1.Set Menu-0A- Traffic type field to PPP. 2.Set Menu-0A Multilink Protocol field to Yes The menus will be configured for MLPPP operations. The bottom menu will display “MLPPP Cfg”
Set WAN bundle connection IP Address	1.Set Menu-0A NET IP address and subnet mask Assign IP address and subnet mask to the bundle link associated to the bundled T1/E1 links. The bundle link is identified as Bundle0 link in all the menus.

Configuring PPP Protocol Parameters

Menu 6-A lets you configure the PPP or MLPPP protocol parameters:

Table 4-8 Menu-6A PPP Configuration

Parameter	Description
Keep alive timer	Controls the messages of the keepalive (echo request) messages after the link(s) is(are) negotiated
Keep alive timeout	Controls how long an end point should wait for “ech response” after ending “echo request”
Retry Counter	How many unsuccessful “echo requests” should be attempted before a link is declared down

Configuring single link Frame Relay

Table 4-9 Configuring Single link Frame Relay

Procedure	
Set router traffic type to Frame Relay	1.Set Menu-0A- Traffic type field to Frame Relay. Set Menu-0A Multilink Protocol field to No
Set WAN port 1 IP address	1.Set Menu-0A NET1 IP address and subnet mask

Configuring independent Frame Relay links

Table 4-10 Configuring independent Frame Relay links

Procedure	Description
Set router traffic type to Frame Relay	1.Set Menu-0A- Traffic type field to Frame Relay. 2.Set Menu-0A Multilink Protocol field to No
Set WAN port 1 IP address	1.Set Menu-0A NET1 IP address and subnet mask
Set WAN port 2 IP address	1.Set Menu-0A NET2 IP address and subnet mask

Configuring Multilink Frame Relay

Table 4-11 Configuring Multilink Frame Relay

Procedure	Description
Set router traffic type to Frame Relay	1.Set Menu-0A- Traffic type field to Frame Relay. 2.Set Menu-0A Multilink Protocol field to Yes The menus will be configured for MLFR operations. The bottom menu will display “MLFR Cfg”
Set WAN bundle connection IP Address	1.Set Menu-0A NET1 IP address and subnet mask Assign IP address and subnet mask to the bundle link associated to the bundled T1/E1 links. The bundle link is identified as Bundle0 link in all the menus.

Configuring Frame Relay DLCIs

Dynamic configuration (LMI)

With Link Management Interface (LMI) enabled on menu-0F, the Dual Trunk E1 Router will automatically discover the configured DLCIs on each of the WAN links.

LMI protocol allows the router to learn the DLCIs from the frame relay switch network. The router will originate and terminate LMI requests and responses.

The Dual Trunk E1 Router support the following three widely used versions of LMI protocol:

- ANSI T1.617 Annex D, referred as Annex D
- ITU Q.933 Annex A, referred as Annex A
- LMI Rev 1.0, referred as Revision 1.0

LMI message types consist of:

- STATUS INQUIRY

  STATUS INQUIRY messages are used to request information on PVCs and their associated DLCIs. These Inquiries can be used to ask the receiving LMI-enabled device about all of the PVCs it knows about. Annex D also supports inquiries about individual DLCIs.

- STATUS

STATUS messages are the replies to Status Inquiries.

The Dual Trunk E1 Router supports both UNI-U and UNI-N

Manual DLCI configuration

You can enter the DLCIs manually in Menu-0E “Performance monitoring cofniguration”. Each DLCI is a sub-interface of a network port (NET1, NET2, or NET). For each DLCI you would enter the Committed Information Rate (CIR), and the remote far end network attached to the DLCI. The delay threshold parameter in the table is relevant only if RMON-1 performance monitoring is enabled.

Mapping DLCIs to IP Addresses

To send IP traffic on a DLCI interface requires address resolution to the next hop IP address. The mapping of of link layer addresses (DLCIs) to the next hop IP address can be done manually (static configuration) or automatically (dynamic configuration) using inverse ARP protocol (RFC2390).

When a DLCI is discovered, the router sends an inverse ARP request to the remote router or edge router. The ARP response messages will trigger the updating of the DLCI to IP Map table.

When a PVC is deleted the table entries associated to the deleted DLCI will are automatically removed. Entries learned through inverse ARP can be deleted manually from the table.

Manual mapping of DLCIs to IP addresses can also be entered in the DLCI to IP Address table from Menu-$IA Frame Relay DLCI IP Map Table.

NOTE: Physical layer loss of signal does not immediately trigger deletion of the dynamically learnt mappings. After loss of signal and failure of LMI retries, LMI status goes down and DLCIs get deleted. At this point mappings are also deleted (made inactive).

CONFIGURING SLIP

SLIP (Serial Line Interface Protocol) is a TCP/IP protocol that allows IP packets to be transmitted over the COMM port. This is configured using Menu 0A - Interface Configuration.

Table 4-12 Configuring COMM port IP address

Procedure	Steps
Set COMM Port IP address	1.Set Menu-0A COMM IP address and subnet mask

CONFIGURING TUI ACCESS RIGHTS

Table 4-13 Setting TUI access rights

Procedure	Steps
Setting normal user password	1.Select menu-8C 2.Select Normal user password field 3.Enter password, 10 characters maximum. A “no passwords” situation gives any user logging on Superuser access rights. By default the normal user password is the same for super user, if no password is set for super user.
Setting super user password	1.Select menu-8C 2.Select Super user password field 3.Enter password, 10 characters maximum If you do set a normal user password, you should set a unique super user password to prevent conflicts.

CONFIGURING RADIUS AUTHENTICATION

When a user telnets to the device, the Dual Trunk E1 Router prompts for user login and password, and sends the request to a designated primary radius server to authenticate the user access. If the server rejects access based on invalid user login or password, or if there is no response received from the server, the Dual Trunk E1 Router will send a ... message to the user and terminates the telnet session. Login failures are logged in the event log.

If the primary server does not respond, after a configured number of retries, the unit can send the request to a designated secondary radius server.

A super user can always bump any existing logged user.

Table 4-14 Configuring Radius authentication

Procedure	Steps
Setting Primary Radius server IP address	1.Select Menu-8G 2.Select Radius Primary Server IP address 3.Enter Radius Primary Server IP address
Setting Secondary Radius server IP address (Optional)	1.Select Radius Backup Server IP address 2.Enter Radius Backup Server IP address
Enter authentication key with Radius Primary server	1. Select Radius Primary Server Secret Key 2.Enter authentication key
Enter authentication key with Radius Backup server	1. Select Radius Backup Server Secret Key 2.Enter authentication key

Table 4-14 Configuring Radius authentication

Procedure	Steps
Configure authentication retries	1. Select Authentication Retries 2.Enter retry count from 1 to 3 If the primary server does not respond, after the configured number of retries, the router will send the request to the secondary Radius server.
Configure authentication response timeout	1. Select Authentication Response Timeout 2.Enter count from 1 to 3

ENABLING/DISABLING TRAFFIC MONITORING

Table 4-15 Enabing/ Disabling Traffic Monitoring

Procedure	Description
Disabling Traffic monitoring	1.Select Menu-0A 2.Set Traffic Monitoring field to Disabled By default Traffic monitoring is Disabled.
Enabling Traffic Monitoring	1.Select Menu-0A 2.Set Traffic Monitoring field to Enabled

CONFIGURING SNMP.

Table 4-16 Configuring Menu-0B SNMP

Procedure	Steps
Setting get community string	1.Select Community get field 1.Enter an alphanumeric text string (max—32 characters). The default setting is public The router SNMP agent uses this text string to check GET requests for the SNMP configuration from the SNMP management station.
Setting set community string	1.Select Community set field 1.Enter an alphanumeric text string (max—32 characters). The default setting is public. The router SNMP agent uses this text string to check SET requests from the SNMP management station to set the SNMP configuration.
Setting trap community string	1.Select Community trap field 2.Enter an alphanumeric text string (max—32 characters). The default setting is public. The router SNMP agent inserts this string in SNMP traps it sends to the SNMP management stations.
Setting First NMS IP addresses	1.Select 1st NMS IP Address field 2.Enter IP address. The router will send trap messages to this server. 3.Select 1st Output Port field 4.Selects the port (COMM, NET, or Ethernet) over which the router will send trap to the 1st NMS IP address. Default port is COMM.
Setting second NMS IP addresses	1.Select 2nd NMS IP Address field 2.Enter IP address. The router will send trap messages to this server. 3.Select 2nd Output Port field 4.Selects the port (COMM, NET, or Ethernet) over which the router will send trap to the 1st NMS IP address.Default port is COMM.

Table 4-16 Configuring Menu-0B SNMP

Procedure	Steps
Setting Third NMS IP addresses	1.Select 3rd NMS IP Address field 1.Enter IP address. The router will send trap messages to this server. 2.Select 3rd Output Port field 3.Selects the port (COMM, NET, or Ethernet) over which the router will send trap to the 1st NMS IP address. Default port is COMM..

CONFIGURING TIME AND DATE SYNCHRONIZATION

Table 4-17 Configuring Time and Date Synchronization

Procedure	Steps
Setting Time server synchronization	1.Select Menu- 2.Set Days, Hours, and Minutes frequency
Configuring Primary Time Server IP Addresse	1.Select Time Src Primary IP Address field 2.Enter Time Server Primary IP address 3.Select physical port of which Time Server is connected to. ENET, ot NET.
Configuring Secondary Time Server IP Addresse	1.Select Time Src Secondary IP Address field 2.Enter Time Server Primary IP address The router accesses both the primary and secondary time servers from the same port.
Enable Time Synchonization	1.Select Automatic Sync field and set it to Enabled. The router Time Client will start synchronizing time and date with the designated Time Server.

CONFIGURING DHCP

Table 4-18 Configuring DHCP

Procedure	Steps
Setting DHCP Server IP address	1.Select Menu-$K 2.Select DHCP server field 3.Enter DHCP Server IP address.
Enabling DHCP Relay agent	1.Select Menu-$K 2.Select DHCP Relay field 3.Set it to Enable to DHCP relay agent.

Bridging Configuration

Overview of the Configuration

The LRU4240 supports bridging and routing packet processing modes. This chapter contains procedures on configuring your device for layer 2 bridging applications.

Bridging provides the capability to connect two or more physically separate LAN segments over the WAN, to create a single logical LAN. Bridging occurs at layer 2 and uses the MAC address assigned to each LAN device, to either forward or filter frames. Routing forwards IP packets between two or more IP networks.

NOTE: With the availability of Bridging mode, the proprietary IP Fast Forwarding mode available in the menu will no longer be supported in the future, and is thereore not documented...

Table 5-1 Bridging configuration procedure

Procedure	Description	Menu	Reference
Setting bridging mode	To configure the unit for Bridging or VLAN Bridging. In bridging mode, all traffic types including IP is bridged.	Menu-$A	page 50
Configuring static MAC Bridge routes	To map statically up to 50 MAC addresses to specific ports in the MAC to port map table. The entries will be stored in non-volatile RAM (NVRAM) and are restored at boot time.	Menu -$GA	page 50
Displaying MAC to port map table	To display the MAC to port map table. View both learnt and static MC to port mapping entries.	Menu -$GB	page 51

Bridging Configuration

Bridging operates at layer 2 of the OSI model to bridge Ethernet traffic between the LAN and the WAN and requires little configuration. All traffic types including IP is bridged. The bridge learns which addresses lay on each side of the bridge and maintains the following information in a MAC to port map table:

- MAC address
- Physical interface (Ethernet or Network ports)
- DLCI, in Frame Relay mode

The MAC to port map table is used by the bridge in its forwarding decisions.

On a Frame Relay connection, using InverseARP, the bridge discovers the remote subnets connected on each DLCI and fills the remote end router's MAC address and the DLCI on which it was discovered.

On the LAN side as packets flow on the Ethernet, the bridge learns which hosts resides on the local LAN by storing the source host address in its MAC to port table.

Whenever a packet destined to a particular MAC address is received, the MAC port map table is consulted, if an entry exists then that packet is transmitted or forwarded on that port. If there are no entry and the packet is received on the Ethernet port, it is forwarded on all the network ports. Incoming packets from the network ports are forwarded over the Ethernet port.

NOTE: Current software release does not implement Spanning Tree algorithm to control and eliminate bridging loops. You will need to avoid bridging loops in your network topology.

Managing the unit in Bridging mode

In bridging mode the unit's Ethernet port IP address is considered the unit IP address, it is the only valid IP address. IP traffic coming from the LAN or the WAN with the destination IP address set to the unit IP address will be processed by the unit as management traffic.

VLAN Forwarding support

The bridge forwards VLAN tagged frames transparently between the LAN and the WAN interfaces. If the unit "Management VLAN ID" is set to disabled, IP packets with the destination IP address matching the unit IP address will be considered as management traffic regardless of the frame's VLAN ID value.

Management VLAN ID

To manage the unit with specific VLAN setting, you will need to set the unit "Management VLAN ID" and "Management VLAN priority" from menu-$A or using the command line interface.

In this case, management traffic is identified by matching the VLAN ID with the unit's Management VLAN ID, and the destination MAC address with the Ethernet port MAC address, or the destination IP address with the unit's port IP address.

Bridging Application Examples

WAN Gateway for IP VPN Application

Connect to your IP VPN over fractional to full E1 circuit using PPP or Frame Relay. For higher bandwidth bond the two E1 links using MLFR or MLPPP, provided your Service Provider supports Multilink Frame Relay or MLPPP services.

The external VPN appliance connected to your LRU4240 initiates and terminates tunnels. The LRU4240 functions as a gateway to your WAN and transfers IP packets at E1 or dual E1 wirespeed.

Point-to-point LAN Extension

Connect two remote LANs over fractional to full E1 circuits transparently using PPP, or Frame Relay on a single DLCI. For higher bandwidth bond the two E1 links using MLPPP or MLFR on Menu-0A.

Multipoint Bridge example

Connect multiple remote LANs over a Frame Relay network. For higher bandwidth bond the two T1/E1 links using MLFR, provided your Service Provider supports Multilink Frame Relay services.

For VLAN applications, a VLAN switch is required for VLAN tagging. The LRU 4240 forwards VLAN tags transparently but does not perform any VLAN tagging.

Configuring Bridging

Table 5-2 Configuring Bridging packet processing mode

Procedure	Description
Setting Bridging over Frame Relay or Multilink Frame Relay	1.Select Menu-0A 2.Set Traffic Type to **Frame Relay** Encapsulation of bridged frames is RFC2427 compliant. In **multilink mode**, the frame header is prefixed with a Multilink Frame Relay header 1.Select Menu-$A 2.Set Packet Processing Mode to **Bridging**. Packets received from the WAN are automatically forwarded to the Ethernet port In bridging mode Menu $ will be reduced to the following menu selections: A.Unit Routing Configuration F. Ethernet ARP Table G. Mac Bridge
Setting Bridging over PPP or MLPPP	1.Select Menu-0A 2.Set Traffic Type to **PPP** 1.Select Menu-$A 2.Set Packet Processing Mode to **Bridging**. Packets received from the WAN are automatically forwarded to the Ethernet port In bridging mode Menu $ will be reduced to the following menu selections: A.Unit Routing Configuration F. Ethernet ARP Table G. Mac Bridge
Enabling Promiscuous mode	By default in Bridging mode the unit is configured with promiscuous mode enabled. This mode allows the unit to receive all packets from the LAN network.
Setting bridging route aging time	Entries in the MAC bridge table are removed automatically when they are inactive for period of time defined as “Bridge Route Aging Time”. By default the aging time is 300 seconds and can be set to up to 1,000,000 seconds. To change the default: 1.Select Menu-$A 2.Set **Bridge Route Aging Time** in seconds The setting will take effect immediately.

Configuring static MAC Bridge Routes

Enter up to 50 entries in the MAC to port map table. The entries will be stored in non-volatile RAM (NVRAM)

and are restored at boot time

Table 5-3 Configuring MAC Static routes

Procedure	Steps
Adding a static MAC bridge entry	1.Select Menu-$GA 2.Select the MAC Address field of an inactive entry 3.Enter the MAC address of the host 4.Select the Interface field 5.Set the Interface field to the physical port **NET-1, NET-2, or ENET-0** This identifies the physical WAN or LAN port on which to bridge the MAC address. 6.Select the DLCI This identifies the logical DLCI on which to bridge the MAC address. 7.Set the `Action` **field to Add**
Deleting a static a static router	1.Select the Action field of the entry you want to delete. 2.Set the `Action` field to **Delete** and press Enter.

Displaying MAC to Port Map Table

The MAC to port MAP table maintains the learnt entries and the static entries . The entries learned are in active state, aged entries are removed from the table automatically. For each entry the menu displays:

- MAC address
- Interface: Enet-0 for Ethernet, NET1, NET2 for network interfaces
- DLCI for Frame Relay connection
- Entry type: **Learned** for entries learned dynamically; **Static** for entries entered manually from menu Menu-$GA; **Self** the unit's Ethernet port MAC address

Table 5-4 Displaying MAC to Port Map table

Procedure	Steps
Displaying **all** MAC to port entries	1.Select Menu-$GB 2.Type **a** for all The menu will display all entries in the MAC to port Map table. Type **n** to view next page Type **p** to view previous page
Displaying **static only** MAC to port entries	1.Select Menu-$GB 2.Type **s** for static 3.The menu will display all entries in the MAC to port Map table Type **n** to view next page Type **p** to view previous page

Figure 5-1

Configuring the Firewall

For instructions on setting the firewall refer to “Configuring the Firewall” on page 61.

Routing Configuration

OVERVIEW OF THE CONFIGURATION

This chapter contains procedures on configuring routing protocols and Network Address Translation. Routing operates at layer 3, uses destination IP addresses and routing table decisions to forward packets to the next hop address..

Table 6-1 Router configuration procedures

Procedure	Description	Menu	Reference
Setting Routing mode	To configure the router to routing mode. In this mode packets will be routed to next hop address based on static and dynamic route tables.	Menu-$A	page 54
Setting default gateway	To specify the default router or next hop where the packet will be forwarded if no routes are found.	Menu-$A	page 54
Configuring static routes	To add, modify, or delete static routes that map destination IP addresses to next hop IP addresses.	Menu-$C	page 55
Configuring Dynamic Routing	To configure RIP1, RIP2, and OSPF dynamic routing protocols through the router CLI.	Menu-$E	page 57
Configuring load balancing with independent links	if more than one route exist to a particular destination, the routing engine will distribute packets equally among the routes with equal cost	Menu-$C	page 57
Configuring NAT	To configure static NAT, dynamic NAT, and overloading.	Menu-$J	page 57
Configuring NAT for single link ISP	To enable NAT for single network link connection to an ISP for internet access.	Menu-$JC	page 59
Configuring NAT for Multihoming	To enable NAT for dual network network links connection to two different ISPs. access.	Menu-$JC	page 60
Configuring NAT for Internet access and Frame Relay network	To enable internet access through central site for remote enterprise networks (Internet backhauling). on a Frame Relay network.	Menu-$JC	page 61

CONFIGURING ROUTING MODE

Table 6-2 Configuring routing mode

Procedure	Steps
Setting routing mode	1.Select Menu-$A 2.Set Packet Processing Mode to Routing Routing mode is global and applies to all supported interfaces.

CONFIGURING DEFAULT GATEWAY

Table 6-3 Configuring default gateway

Procedure	Steps
Setting default Gateway IP Address	1.Select Menu-$A 2.Select Default Gateway IP Address field 3.Set IP Address
Enabling default gateway	1.Select Menu-$A 2.Set Default Gateway to Enabled

CONFIGURING STATIC ROUTES

Static routes lets you define a route that maps the destination IP address received in a datagram to an egress port or a next hop IP address. A subnet mask is also configured to specify which portion of the destination IP address is the destination network address portion

```
SW Ver 1.22RT MIB Ver 1.21  Black Box Dual Trunk E1 Router           10/18/02
HW Ver A   ID:                     Menu-$ Routing Configuration       15:17:49
                      $C. Static Routing Table

 Status     Destination IP/Len      Next Hop IP  Interface  Metric    Action
----------------------------------------------------------------------------
Inactive          0.0.0.0 /16          0.0.0.0    Unknown       0   Delete
Inactive          0.0.0.0 /16          0.0.0.0    Unknown       0   Delete
6 Inactive      1 0.0.0.0 /16        2 0.0.0.0  3 Unknown     4 0   Delete 5
Inactive          0.0.0.0 /16          0.0.0.0    Unknown       0   Delete
Inactive          0.0.0.0 /16          0.0.0.0    Unknown       0   Delete
Inactive          0.0.0.0 /16          0.0.0.0    Unknown       0   Delete
Inactive          0.0.0.0 /16          0.0.0.0    Unknown       0   Delete
Inactive          0.0.0.0 /16          0.0.0.0    Unknown       0   Delete
Inactive          0.0.0.0 /16          0.0.0.0    Unknown       0   Delete
Inactive          0.0.0.0 /16          0.0.0.0    Unknown       0   Delete

                                Page  1 of 15
------------------------------------------------------------------------------
0-IP Cfg    1-Main Status   2-Enet Status  3-Reports 4-Main Cfg  5-N/A
6-MLPPP Cfg 7-Feature Keys  8-Alarm/Misc   9-Diagnostics         $-Routing
n-Next page                               p-Previous page
CR-changes a selection                    Arrow keys-move selection
```

Table 6-4 Configuring static routes

Procedure	Steps
Adding a static route	1.Select the Destination IP field of an inactive route 2.Edit the IP address 3.Select the Len field 4.Enter the subnet mask value of the destination network. Value 0 to32. The subnet mask is determined by the number of 1's left justified in a 32-bit submask field, with the rest of the field set to zeros. The subnet mask describes how many bits in the destination IP network address are valid, and are to be matched against incoming packet's destination address. 5.Select the Next Hop IP field 2 or select the Interface field 3 to enter either the IP address for routers on numbered interfaces or to enter the egress port. Enter the IP address for routers on numbered interfaces (Ethernet). This is the IP address of the router where incoming matching destination IP packets are sent. This IP address must be on the same subnet as one of the numbered ports. Or Set the egress port to either NET1, NET2, ENET-0, Bundle0. This identifies the physical WAN or LAN port associated to the route. 6.Set the `Metric` **field** 4 The metric specifies the route cost. Enter a number between 1 and 255 to define the hop count. Use this count to create preferential hops for prioritizing routing entries. If more than one route of equal cost is found for a particular destination, the routing engine will distribute the packets equally among the available routes using a round-robin algorithm. See "Setting the Metric parameter for Load Balancing" below. If multiple routes are found with unequal costs then the route with lesser cost metric is chosen. 7.Set the `Action` **field** 5 **to Add** If this new route is accepted by the routing engine the status field 6will change from Inactive to Active. If the route is not accepted, the action field 5 will change to Modify. You will have to change one of the settings in the route and try to add it again.

Table 6-4 Configuring static routes

Procedure	Steps
Modifying a static router	1.Select the Action field of the route you want to modify. 2.Select Modify The status of the first column will change to Inactive. You can now select and change any parameter of the selected static route. 3.Modify the `destination IP` field 1. 4.Modify the `Next Hop IP` field 2 or Modify the `Interface` field 3. 5.Modify the `Metric` field 4 6.Set the `Action` field 5 to Add and press Enter. If the modified route is accepted by the routing engine, the status field 6 will change from Inactive to Active. If the modified route is not accepted, the action field 5 will change to Modify. You will have to change one of the settings in the route and try to add it again.
Deleting a static route	1.Select the `Action` field 5 of the route you want to delete. 1.Select Delete command The status of the first column will change to Inactive and the action field will be set to Delete.

Load balancing over independent links

To load balance traffic between two E1 links to a remote network, you will need to set two routes with equal cost. Both routes will have the same destination network and different interface (NET1, NET2).

CONFIGURING DYNAMIC ROUTING

The dynamic routing protocols RIP1, RIP2, and OSPF are configured using the command line interface accessible from Menu-$E. The router CLI commands and parameters are documented in appendix E.

NOTE: Standard LRU4240 includes RIP1, RIP2, and OSPF dynamic routing. BGP-4 protocol is available as an optional dynamic routing protocol.

CONFIGURING NAT

NAT allows the use of private IP addresses when accessing the Internet. Any host with unregistered IP address must use NAT to communicate with the rest of the world. This service is transparent to the internal local hosts.

In this documentation “Local” refers to unregistered IP addresses and “Global” refers to registered IP addresses.

NAT bindings can be done statically, where a given local host may always map to a given global address, or dynamically where the router assigns to the local host accessing the internet a global address from the pool addresses given by the ISP.

The Dual Trunk E1 Router supports the following NAT features:

- Static NAT - To map a unregistered IP address to a registered IP address. This is useful to enable outside hosts to access an internal IP host of server.
- Dynamic NAT - To share dynamically a range of global addresses among internal hosts to access the internet. Translation occurs when traffic takes place.
- Overloading - If the number of global addresses available is less than number of hosts which need to access internet at the same time, then the port field also can be used for translation. Unregistered IP addresses are mapped to one or many registered IP addresses.

NAT Configuration menus

NAT is configurable through the TUI menu $J accessible direcly or remotely via Telnet.

Table 6-5 NAT configuration menus

Menu	Description
Menu-$JA Global Map table	To configure the global IP address ranges to allocate through NAT.
Select **Add** command	Add the global IP addresses to NAT.
Menu-$JB NAT static table	To configure the one-to-one mapping of global IP addresses to local IP addresses.
Menu-$C-Local address table	To configure the networks that require NAT translation. If the table is empty no NAT translation will take place. NAT will translate if the packet source or destination IP address is included in the Local table. NAT will not translate if both the packet source AND the destination IP addresses are included in the local table. This is useful for network scenarios where filtering NAT, based on source and destination addres, is required.
Menu-$JE NAT Interface configuration	To enable or disable NAT and NAPT per WAN interface.
Menu-$JF NAT Dynamic entries	To verify dynamic operations. You can view the dynamic alloction of global IP addresses to local host as traffic takes place.

Configuring NAT for single link ISP

Use the following procedure to configure your Dual Trunk E1 Router with dynamic NAT for internet access to a single ISP

Table 6-6 Configuring NAT with single link ISP

Procedure	Steps
Setting single link NAT ISP to NET1	Example: You were assigned 14 global IP addresses starting from 100.120.30.02 by your ISP for NET1 1.Select menu-$JAGlobal Map Table 2.Select **Translated IP address** field. 3.Enter 100.120.30.02 as the starting global IP address 4.Select subnet mask 5.Enter 28. 6.Set the interface field to NET1 Select the interface on which the network is connected to the ISP. With 4230 Access Router select NET1. With 4240 Dual Link Router select either NET1, NET2, or Bundle0 7.Set Action field to Add
Enter local networks that require NAT translation	1.Select Menu-$JC Add a row entry in this table for each network you want enable internet access. 2.Select local IP address field of an inactive entry (field set to Delete) 3.Enter the IP address that will be translated 4.Set subnet mask field of the translated network 5.Select interface field 6.Select the connection the translated network is connected to. Enet0 for directly attached network NET1, NET2 or Bndl0 for remotely attached network via WAN port.
Optional - Enable overloading	If you want to share a single global IP address or a range of global IP addresses among multiple host. 1.Select menu-$JE 2.Set NAPT field to Enabled on the global interface (the network interface through which the global networks can be reached, NET1 in this example)
Enable dynamic NAT	1.Select menu-$JE 2.Select unit NAT field and set it to enabled 3.Select the global network interface (NET1 in this example) NAT field and set it to Enabled

Single link Internet Example

In this typical branch office configuration, a single global IP address is shared by multiple hosts when accessing the internet via the 4230 single T1/E1 .

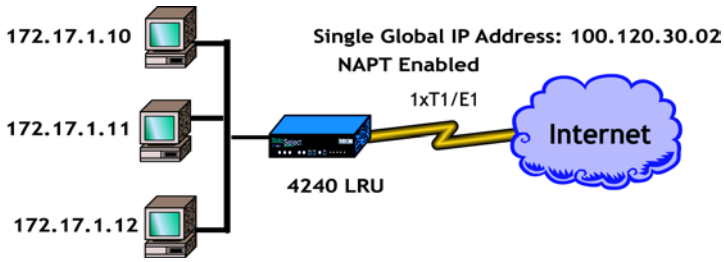


Figure 6-1 NAT single link application example

Table 6-7 Single link Internet Access configuration

Procedure	Steps
Setting single link NAT ISP to NET1	1.Select menu-$JAGlobal Map Table 2.Set **Translated IP address** field to 100.120.30.02 3.Set **subnet mask** to 32 4.Set the interface field to **NET1** 5.Set Action field to Add
Enter local networks that require NAT translation	1.Select Menu-$JC 2.Select the first row in the table 3.Set **Local IF IP Address field** to 172.17.1.0. This is the subnet that will be translated when accessing the internet 4.Set subnet mask field to 24. Assuming the network id is 172.17.1 5.Set **Interface** field to **Enet0** 6.Select the connection the translated network is connected to. Enet0 for directly attached network
Enable dynamic NAT and overloading	To share the single global IP address among the multiple hosts. 1.Select menu-$JE 2.Select the NET1 row in the table 3.Set NAT field to **Enabled** 4.Set NAPT field to **Enabled** 5.Set Two Way NAT to **Disabled** . (Default setting) **Note:** Leave all the fields for both ENET row and NET2 to disabled

Configuring NAT for Multihoming

Use the following procedure to configure your Dual Trunk E1 Router for multihoming, internet access to two ISPs simultaneously. In the example we'll configure:

- NET1 to ISP1 with single global IP address 120.20.30.10
- NET2 to ISP2 with 4 global IP address starting from 200.80.100.21.

Table 6-8 Configuring NAT for Multihoming

Procedure	Steps
Setting ISP1 link	1.Select menu-$JAGlobal Map Table 2.Select **Translated IP address** field. 3.Enter 120.20.30.10 as the starting global IP address 4.Set subnet mask to 32 5.Set the interface field to NET1. 6.Set Action field to Add
Enter local networks that require NAT translation on NET1	1.Select Menu-$JC Add a row entry in this table for each network you want enable internet access. 2.Select local IP address field of an inactive entry (field set to Delete) 3.Enter the IP address that will be translated 4.Set subnet mask field of the translated network 5.Set interface to NET1
Setting ISP2 link	1.Select menu-$JAGlobal Map Table 2.Select **Translated IP Address** field. 3.Enter 200.80.100.21 as the starting global IP address 4.Set subnet mask to 30. This will allocate addresses: 200.80.100.21 through 24 5.Set the interface field to NET2. 6.Set Action field to Add
Enter local networks that require NAT translation on NET2	1.Select Menu-$JC Add a row entry in this table for each network you want enable internet access. 2.Select local IP address field of an inactive entry (field set to Delete) 3.Enter the IP address that will be translated 4.Set subnet mask field of the translated network 5.Set interface to NET2

Configuring NAT for Internet access and Frame Relay network

In the example below the enterprise frame relay network central site provides internet access for all the remote enterprise networks. A single DLCI (200) will be set for Internet access. The central site router will be configured to:

- Disable NAT on intranet traffic. IP traffic between central site networks and remote branch networks will take place without any NAT translation. This will enhance the router performances.
- Enable NAT on internet access. NAT translation will take place on any internet traffic from central network or remote networks.

Table 6-9 Configuring bundled internet access and Frame Relay network

Procedure	Steps
Setting ISP1 link	1.Select menu-$JAGlobal Map Table 2.Select **Translated IP address** field. 3.Enter 120.20.30.10 as the starting global IP address 4.Set subnet mask to 32 5.Set the interface field to NET1. 6.Set Action field to Add
Enter the central site and remote network	1.Select Menu-$JC Add a row entry in this table for each network you want enable internet access. 2.Select local IP address field of an inactive entry (field set to Delete) 3.Enter the IP address that will be translated 4.Set subnet mask field of the translated network 5.Set interface to NET1

Firewall Configuration

The Firewall table is an access list that filters packets by denying or permitting access from source hosts to destination hosts. The rules are applied according to the order set in each entry in the list. The first match determines whether or not the packet is accepted or denied by the router. If a packet passes a first match and is not denied access, subsequent rules are applied on the packet. The default access setting is to deny all access.

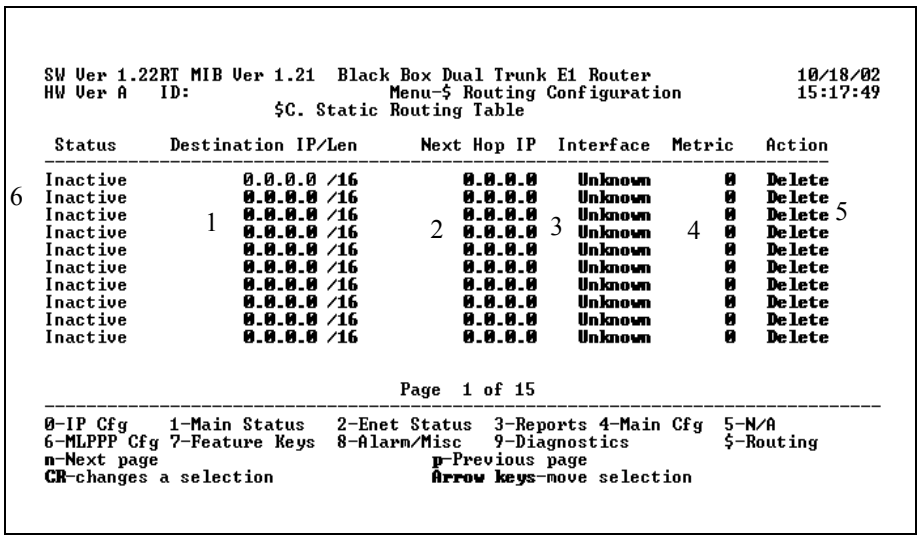
..

Table 7-1 Router configuration procedures

Procedure	Description	Menu	Reference
Configuring Firewall	The Firewall table lets you set an access list of up to 150 entries to permit or deny access based on the source or destination IP addresses. The default Firewall setting is to deny all access.	Menu-$H	page 63

CONFIGURING THE FIREWALL

You need to enable first the Firewall on menu $A, before you activate entries in the Firewall table.



To add an entry to the access list:

Table 7-2 Configuring Firewall

Procedure	Steps
Adding or modifying an entry	1.Select the `Ord` field 1 of an inactive route line. 2.Enter an order number between 0 and 511. The firewall uses a rule based order of execution. This identifies the order of execution of the entry in the firewall table. 3.Set the `Action` field 2 to either Deny or Permit. 4.Enter in the `Src Address/Len` field 3 the IP address and subnet mask of the host you want to permit or deny access from. 5.Enter in the `Dest Address/Len` field 4 the IP address and subnet mask of the host you want to permit or deny access to. 6.Set the `SrcIntf` field 5 to PPP1, PPP2, or ENET-0. Src Interface specifies the interface on which the packet was received. 7.Set the `Status` field 6 to Active 8.Save and activate the entry by pressing k Entries in the list will be ordered according to the order and the pairs of source and destination.
Deleting or deactivating an entry	1.Select the `Status` field 6 of the selected active route. 2.Set the `Status` field to Inactive

Diagnostics

The Dual Trunk E1 Router offers extensive diagnostic capabilities for local and remote analysis. These include fixed test patterns and two user-programmable 24-bit test patterns. In addition to front panel LEDs, the Dual Trunk E1 Router features more than a dozen user-configurable parameters and performance thresholds for remote alarm reporting.

Required Tools and Equipment

Obtain the following tools and equipment when performing the procedure(s) to isolate the Dual Trunk E1 Router from the network:

- A standard E1 test set, such as a FIREBERD 6000 or equivalent with a E1 Interface and cables.
- An RJ-48 plug connector with two patch cords for connecting to the E1 test set.
- Protocol analyzer or FIREBERD 500 to capture and analyze PPP protocol layer. Third party software protocol analyzer tools on PC to use as standard data test set, to capture packets on the Ethernet layer such as EtherPick, or Snoop command on Unix.
- Hand tools for attaching and removing cables.

If you do not have any test equipment, you must rely on the network to do most of the troubleshooting for you.

Performing Tests from the Front Panel

Using the arrow keys on the front panel, you can perform the following tests. For more information on front panel controls, see Chapter 3, *"Terminal Setup."*

- Self Test
- Loopback Tests
- Pattern Tests
- Lamp Test

Self Test

The Self Test checks the unit's electronic components and performs a signal path check of transmit and receive directions simulating a 4000-ft E1 line.

The messages are `RUNNING SELFTEST, SelfTest Successful`, or one of the error messages listed in Table 8-1.

Table 8-1 Self Test Indicators

Indicators	Description
Flash Code Error	CRC of flash copy of executing code failed.

Table 8-1 Self Test Indicators

Indicators	Description
DRAM CRC Error	CRC of RAM copy of executing code failed.
Flash Boot Error	CRC of flash boot code failed.
Flash Loader Error	CRC of flash factory loader failed.
Net Error	Pattern test failed.
Flash Write Error	Flash write test failed.

Loopback Tests

You can isolate sections of the Dual Trunk E1 Router to determine if it is defective. The problem is normally in the network.

This section describes each of the loopback tests you can perform from the Dual Trunk E1 Router's front panel. The tests are:

- Loop NET 1/2
- Loop Payload
- Loop Up Remote and Loop Down Remote

NOTE: No test is 100% complete and a small portion of the network will remain untested. Your unit may allow only one active loopback at a time.

NOTE: In the figures that illustrate the available tests, the path for only one Port (Link) is shown, to prevent overly confusing drawings. If the test is also being run on the second port, its path will be similar to that shown in the figure.

Loop NET Test

The Loop NET test, illustrated in Figure 8-1, verifies the operation of the E1 network and is available only on full bandwidth.

This test loops the data received from the network back to the network. The data is regenerated before it is looped back; however, the unit does not perform additional processing of the data. This minimizes the impact of the unit during the test so that network problems can be isolated.

This test can loop Net1, Net2, and All Nets.

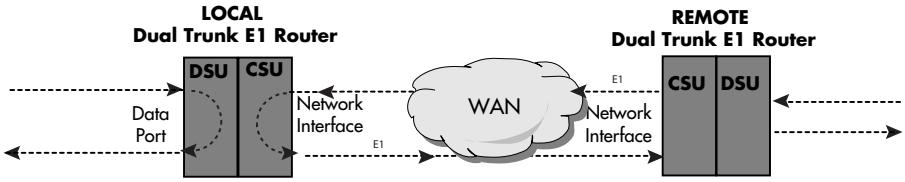


Figure 8-1 Loop NET Test

Loop Payload Test

The Loop Payload test verifies proper operation of the unit and the network.

This test loops the payload data received from the network back toward the network. Before it is looped back, the data is regenerated and a new framing pattern is inserted. Thus, the proper E1 framing of the Dual Trunk E1 Router and network can be verified.

This test can loop Net1, Net2, and All Nets.

Loop Up Remote and Loop Down Remote Tests

The Loop Up/Down Remote test, illustrated in Figure 8-2 on page 8-68, places the remote unit into Network Loopback using the industry standard set codes. Once in Network Loopback, test patterns can be sent to verify the Bit Error Rate (BER) performance of the bi-directional E1 network signal.

To place the remote unit into network loopback, the local Dual Trunk E1 Router continuously transmits the industry standard loop up code to the remote unit. If the remote unit does not go into network loopback within 15 seconds a failure is declared and the Dual Trunk E1 Router stops sending the loop up code.

The loop code and network parameters for the local and remote units must match.

Use the Loop Down Remote test to terminate the remote loopback. This test can be used no matter how the remote unit was put into loopback.

Perform the Loop Up Remote and Loop Down Remote tests from the front panel, user interface or SNMP.

This test can loop Net1 and Net2, but not All Nets.

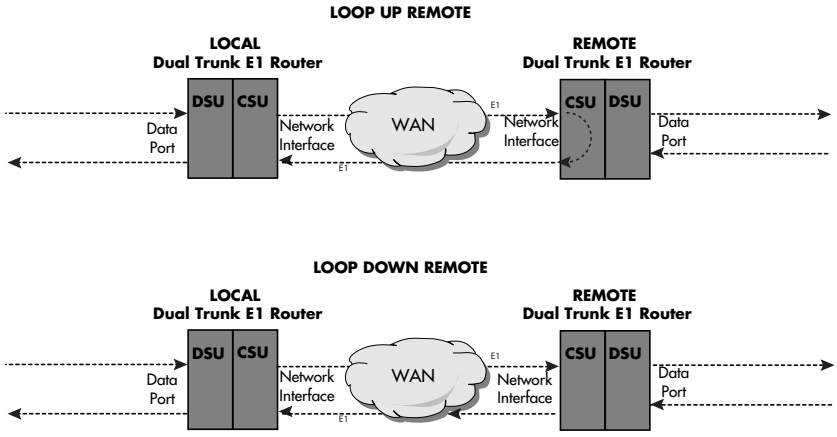


Figure 8-2 Loop Up/Down Remote Test

NOTE: The full bandwidth loop up code puts the remote Dual Trunk E1 Router in a full bandwidth ***network*** loopback.

Pattern Tests

QRW Pattern Test

Use the Quasi-Random Word (QRW) test to measure Bit Error Rates on the network. The Dual Trunk E1 Router sends a QRW pattern into the network and monitors the received E1 network signal for QRW bit errors. QRW is a good approximation of actual user data. It is also known in the industry as Quasi Random Signal State (QRSS).

This test also looks for bit errors in both E1 circuit directions when the remote system is looped up. In this case, the system transmits the QRW to the E1 network; the remote system loops it back to the Dual Trunk E1 Router which monitors the signal for errors.

You can also use the QRW code to isolate a E1 network problem to a specific transmission direction. In this case, both E1 transmission directions are monitored when the local and the remote system transmit QRW (the remote is not put into loopback).

Other Pattern Tests

Other pattern tests types are listed and described in Table 8-2.

Table 8-2 Send Test Types Descriptions

Send Test Type	Pattern Test Description
1:7 Pattern	Stresses the timing recovery circuits of repeaters and other intermediate equipment.
1:1	Sends alternate ones and zeros—used to test for bridge taps.
All Ones	Used for signal power measurements.

Table 8-2 Send Test Types Descriptions

Send Test Type	Pattern Test Description
All Zeros	Used for verification of B8ZS.
1:4 (or Alternate)	The 1:4 code is the loopup remote code. Typically, it is used when the loopup remote test fails to place the remote system into loopback. You can determine if the failure is an intermittent or a hard failure by continuously sending the 1:4 code, and monitoring the network status to see if the pattern is being received. The selections are available on the full link and on NET 1 and NET 2. **Note**: If the Loop Up Remote test fails to place the remote system into loopback, check that the Loop Code and Network Framing parameters are the same at each end of the link.
1:2	The 1:2 code is the loop down remote code. Use it when the Loop Down Remote test fails to terminate the remote loopback. You can determine if the failure is an intermittent or hard failure by continuously sending the 1:2 and monitoring the network status to see if the pattern is being received. The selections are available on the full link and on NET 1 and NET 2.
User 1/User 2	These two user programmable patterns (up to 24 characters) let you create a test pattern rather than use pre-programmed patterns.

Lamp Test

Use this test to verify the LEDs. During the test, all LEDs on the front panel illuminate.

PERFORMING DIAGNOSTICS FROM THE TERMINAL

Menu-9 Diagnostics

Menu-9, Diagnostics, provides access to diagnostic testing screens and monitoring configuration screens. Any test described in "Performing Tests from the Front Panel" on page 65 can also be performed from the terminal screen menus.

You can run several tests from your system's internal diagnostics, shown in Menu-9, Diagnostics.

- Menu 9A — Physical Layer Diagnostics
- Menu 9B — Link Layer Diagnostics
- Menu 9C — Delay Monitoring Configuration

Menu-9A Physical Layer Diagnostics

This section describes the Menu-9A parameters and tests.

To verify connections and the E1 line, run the basic diagnostic and pattern tests from Menu-9A, Physical Layer Diagnostics.

Performing a Test from Menu-9A Physical Layer Diagnostics

To run a test from Menu-9A, Physical Layer Diagnostics:

1. **Select the test and the port number in the Test field and set the Test length, USER1 and USER2 Pattern fields.**
2. **Follow the screen prompts.**

Test results are shown in the upper portion of the screen.

The selections for ports on which the test is performed are Net1, Net2, and on some tests, All Net. Port is ignored with the Self Test, or Lamp test.

The Inject A Pattern Error option (to inject a single-bit error) is available only when the unit is sending a test pattern.

PERFORMING DIAGNOSTICS FROM TELNET

NOTE: Performing a test can cut off existing Telnet connections on the Ethernet and the NET Port. Since certain tests can cut off Telnet connections, only a subset of tests can be selected when the user logs onto the Dual Trunk E1 Router by Telnet through the NET Ports.

Certain tests prevent the Telnet session from being disrupted when you Telnet into the unit. Tests that can be run through a Telnet connection are listed in Table 8-3.

Table 8-3 Tests Allowed Through Telnet Connection

Test	COM	NET
Self Test	Yes	Yes
Loop Net	Yes	No
Loop Payload	Yes	No
Loop Up Remote	Yes	No
Loop Down Remote	Yes	No
QRW Pattern	Yes	No
1:7 Pattern	Yes	No
3:24 Pattern	Yes	No
1:1 Pattern	Yes	No
All 1s Pattern	Yes	No
All 0s Pattern	Yes	No
1:2 Pattern	Yes	No
1:4 Pattern	Yes	No
User 1 Pattern	Yes	No
User 2 Pattern	Yes	No
Lamp Test	Yes	Yes

NOTE: You do not need to notify the telephone company that you are running the tests. However, if the tests reveal a problem with telephone company service or with the Dual Trunk E1 Router, you should inform the telephone company that the Dual Trunk E1 Router must be removed from service.

When performing a test, you can:

- Initiate loopbacks and tests on full bandwidth or on NET 1 or NET 2.
- Set programmable test patterns

Link Layer Diagnostics and Delay Monitoring

When installing or maintaining wide area connections, you must verify the end-to-end operation of the WAN links. With dedicated E1 line, you can verify the WAN link by placing the Dual Trunk E1 Router on one end of the line in a loopback test and initiating the transmission of a pattern test from the other end. The pattern is received and monitored to detect transmission errors.

Link-based Testing for Public Packet Networks

The link-based testing feature qualifies and tests PPP-based networks non-intrusively. Using the ICMP ping packet, the unit adds pattern generation and packet sequencing that allows single-ended and collaborative testing. This lets the user test his network from one end to the other using any TCP/IP-based test equipment. Link-based testing encapsulates a BERT pattern inside an ICMP message that the remote Dual Trunk E1 Router reflects. The packet can then be directed to test the network, or LAN port. Patterns supported include 511, 1023, 2047, all 1s, all 0s, and alternating 1s and 0s.

Delay Monitoring for TCP/IP

The delay monitoring feature provides network delay measurement beyond the link between the Dual Trunk E1 Router and any IP-addressable device on the network. Blackbox measures delay by using ping packets, which timestamp and obtain round-trip delays to specific IP addresses. The traffic added to support the measurement is minimal, and the user can configure the frequency. The length of the ping packet can allow delay measurements at different frame sizes. A user who is concerned about bandwidth taken away by the measurement can configure the test for a single, short ping every few minutes, making the test bandwidth penalty virtually non-existent.

The link-based testing and delay monitoring features allow network managers to test links and quantify delays, and are especially useful during network installation and trouble isolation. Both features provide the benefit of circuit-level testing across the network.

Non-Disruptive Testing

The Link Layer Diagnostics and Delay Monitoring are non-disruptive to normal traffic. Unlike hard loopback tests that affect the line, Link Layer Diagnostics do not take the line out of service.

Depending on the link speed and the test specified, Link Layer Diagnostics uses some of the bandwidth that would otherwise be available for payload. This bandwidth reduction is negligible if the test is specified with short and infrequent packets.

On point-to-point networks Link Layer Diagnostics do not disrupt payload traffic.

Menu-9B—Link Layer Diagnostics

Link Layer Diagnostics uses an encapsulated Bit Error Rate Test (BERT) pattern inside ping messages and reflects the BERT pattern from the remote unit.

1. **Select a pattern test.**
2. **Select the IP address of the equipment to send the PING message.**

   Select the local or remote router, or the remote Dual Trunk E1 Router.
3. **Select a port to test.**

   Ports are NET, Ethernet, and COM.
4. **Select the Test Interval**

   Select time in seconds between 2 ping messages.

5. **Select the Test Length:**

   The length of the test can be smaller than the time between two ping messages as specified in the previous step. If it is, only one ping is sent.

6. **Select the test packets length.**

   From the minimum to the maximum allowed packet length (0 byte to 1500 bytes).

7. **Press S to start the test**

   The Dual Trunk E1 Router begins sending ping messages at the specified intervals.

Press the **E** key to terminate the test at any time.

The results of this test are:

- Number of packets sent
- Number of packets received
- Number of errored packets
- Number of missing packets
- Average round trip delay

MONITORING AND MANAGEMENT

The Dual Trunk E1 Router collects and displays performance data and other data useful for network troubleshooting. The Dual Trunk E1 Router monitors the E1 line continuously and displays all collected data on the terminal screen.

This chapter describes how to monitor the unit status, display performance reports, and configure alarm conditions.

You can monitor and manage the unit from a terminal, remote terminal Telnet connection, or an SNMP management station. In addition, if in–band management is enabled, you can monitor and manage the Dual Trunk E1 Router inband through a Telnet connection or an SNMP network management station.

The terminal interface has menus which enable you to:

- Display or modify the unit configuration. For more information, refer to "Overview of the Configuration" on page 33.
- Configure alarm conditions, passwords, and modem connections. For more information, refer to "Configuring Alarm Conditions" on page 85.
- Monitor the status of the unit and the Data Port. For more information, refer to "Menu-2 Data Status" on page 80.
- Monitor the Dual Trunk E1 Router performance database. For more information, refer to "Displaying Performance Reports" on page 76.
- Run diagnostic tests. For more information, refer to "Troubleshooting the Unit" on page 87

Terminal User Interface Access Methods

Below is a brief review of how to access your Dual Trunk E1 Router for monitoring your unit for running tests.

- Super User versus normal user access rights. For more information, refer to "Configuring Access Rights" on page 32.
- Logging on or off from a terminal. For more information, refer to "Logging On from a Terminal" on page 30.
- Logging on from a Telnet connection. For more information, refer to "Logging on from a Telnet Connection" on page 31.

MONITORING PERFORMANCE

Each Dual Trunk E1 Router collects and displays performance data as well as additional parameters to help you troubleshoot problems. To manage and monitor the Dual Trunk E1 Router, use Menu-3, Reports, to display the unit's performance reports, which are described further in this chapter. Additionally, reports on overall link utilization over a variety of intervals are available from Menu 3.

Displaying Performance Reports

Several types of performance reports are available. Select a report in Menu-3, Reports. Type the corresponding letter or use the up and down arrow keys to move through the menu and press **`Return`** to select the report.

The first two reports display the carrier and user registers respectively. The carrier registers are the same as those reported over the FDL in response to FDL requests and can be cleared only by the carrier.

NOTE: The maximum error count displayed in performance reports is 65,535. The actual value may be higher.

Table 9-1 and Table 9-2 provide a comprehensive list of events and descriptions used in the Performance Reports. For more information, see Menu 3 and its sub menus.

Performance Report Menus

Table 9-1 Performance Report Menus

Menu Screen	Description
3AA - Carrier Registers, Current Interval	Displays performance data for the most current 15-minute interval.
3AB - Carrier Registers, 24 hour total	Displays performance data for the last 24-hour period.

Table 9-1 Performance Report Menus

Menu Screen	Description
3AC - Carrier Registers, 24 Hour Detail	Displays performance data organized in 96 15-minute intervals.
3AE - Carrier Registers, 4 day Detail	Displays performance data for every 15-minute interval in the last 4 days. (up to 32 screens)
3AF - Carrier Registers, 14 Day Summary	Displays performance data totals for each day, for the last 14 days
3AG- Carrier Registers, uptime total	Displays performance data total for uptime interval.
3BA - User Registers, Current Interval	Displays performance data for the current interval.
3BB - User Registers, 24 Hour Total	Displays performance data for the last 24-hour period.
3BC- User Registers, 24 Hour detail	Displays performance data organized in 96 15-minute intervals
3BE - User Registers, 4 day Detail	Displays performance data for every 15-minute interval in the last 4 days. (up to 32 screens)
3BF - User Register, 14 Day Summary	Displays performance data totals for each day, for the last 14 days
3BG - User Register, uptime total	Displays performance data total for uptime interval.

Performance Data Report Events

Table 9-2 Menu-3 Performance Data Report Events

Event	Description
Unavailable Signal State	This state is declared at the onset of ten consecutive SESs.
Payload Loopback Actuated	The unit is in Payload Loopback.
Current Interval Timer	Displays the amount of time in a current interval, 0 - 899 seconds.
Errored Seconds (ES)	A second with one or more CRC or CRC-4 errors.
Unavailable Seconds (UAS)	The number of seconds elapsed after 10 consecutive SES events are received.
Severely Errored Seconds (SES)	A second during which 832 or more CRC-4 violations or OOF events have occurred.
Loss of Frame Count (LOFC)	The number of times Loss of Frame is declared.
Controlled Slip Seconds (CSS)	The number of seconds in an interval in which a controlled slip occurred.
Background Block Error	(Background block errors/number of available blocks)*100. Number of available blocks is (number of available seconds)*1000.

Event Log

The Event Log feature is accessed through Menu-3Z. The Event Log is a running list of system events such as power on, power off, errors, configuration changes, and test status. When you access the Event Log, this information is displayed in a table as each even occurs. A complete list of events indicated by the Event Log are given in the Menu 3Z.

ROUTING MONITORING

The Dual Trunk E1 Router collects statistics on the following:

- Ethernet physical layer
- Data ethernet
- IP MIB Statistics

Table 9-3 Routing Report Menus

Menu Screen	Description
3FA - Ethernet physical layer	Displays the ethernet protocol statistics which includes FCS errors, total single collision frames, total number of deferred transmissions, total number of late collisions, total number of carrier sense errors, and total number of frames received that are too long.
3FB - Ethernet interface statistics	Displays data ethernet statistics which include totals for octets received/transmitted, unicast packets received/transmitted, non unicast packets received/transmitted, number of packets received with unknown protocol IDs, RX packets received with Ethernet errors, and non-routable RX packets received.
3FC - IP statistics	Displays IP MIB statistics including: totals packets received
3FE - ICMP Receive statistics	Displays performance data for every 15-minute interval in the last 4 days. (up to 32 screens)
3FF - ICMP Transmit statistics	Displays performance data totals for each day, for the last 14 days
3FG - ARP statistics	Displays performance data uptime totals for the NET1, NET2, and aggregate network port

DELAY MONITORING

The delay monitoring feature in the Dual Trunk E1 Router provides network delay measurement between the Dual Trunk E1 Router and any device on the network. The LRU4240 measures delay by using a ping protocol. As part of the pattern generation and packet sequencing, delay measurement will use the ping packet to timestamp and obtain round-trip delays to specific IP addresses. This method can measure the delay to any device that implements the TCP/IP protocol, not just to BlackBox units. The traffic added to support the measurement is minimal, and the user can configure traffic frequency. The length of the ping packet can allow delay measurements in different frame sizes. A user who is concerned about bandwidth utilization by the measure can configure the test for a single short ping every few minutes, making the test bandwidth penalty virtually non-existent.

The link-based testing and delay monitoring features allow network managers to test network links, as well as quantify the network delay, and are especially useful during network installation and trouble isolation. Both features provide the benefit of circuit level testing across the network.

Menu-9C allows you to configure the Dual Trunk E1 Router for delay monitoring. The results of the test are displayed in Menu-3M.

MONITORING STATUS

You can monitor the status of the Dual Trunk E1 Router unit from Menu-1, Main Status, and the status of the single data port from Menu-2, Data Status.

Transmit and receive directions are monitored separately by the unit. The overall link utilization is reported in Menu-1, Main Status, and the report is updated once per second in each direction.

Menu-1 Main Status

You can monitor the status of the Dual Trunk E1 Router from Menu-1, Main Status. This menu presents information on unit status, network status, and Ethernet port status.

Main Status Fields

All fields in Menu-1 are read-only.

Unit Status

The Unit Status indicates the Dual Trunk E1 Router is operating normally, or if any special conditions exist.

Net 1/Net 2 Network Status

The Network Status field presents information on the condition of the received E1 signal.

Data Ethernet Status

Link up and Link down

Clearing Error Counters

1. **To clear the error statistics counters, press `C`.**

   ```
   Do you really want to clear the error counters (Y/N)
   ```

2. **Press `y` to confirm, or press any other key to take no action.**

Menu-2 Data Status

Menu-2, Data Status, shows the current status of the Ethernet port, it will indicate “Link up” or “Link down”.

IN–BAND MANAGEMENT

The unit’s in–band management feature provides an easy way to manage Dual Trunk E1 Router network devices through the data path. This feature eliminates the need for external hardware (i.e., serial cable), terminal server, Ethernet hub port, or router AUX port connection to manage the unit.

In-band Network Registers, 24 Hour Detail

On an in-band enabled system, Menu-3CB shows the performance data which describes l

Table 9-4 Menu-3CB Field Definitions

Field	Definition
CRC	Number of packets received with CRC errors per interval.
RxPkt	Number of received packets per interval.
Rx%	Bandwidth utilization in the received direction per interval.
TxPkt	Number of packets sent out per interval.
Tx%	Bandwidth utilization in the transmit direction during interval.

RMON-2

RMON-2 provides additional SNMP reporting capabilities and the ability to identify the top bandwidth users.

When using RMON-2 with the Dual Trunk E1 Router, the following RMON-2 groups are available:

- Protocol Directory
- Protocol Distribution
- Network Layer Host Table
- Application Layer Host Table
- Network Layer Matrix Table
- Application Layer Matrix Table

Protocol Directory

The RMON-2 Protocol Directory lists the protocols that the Dual Trunk E1 Router (agent) is monitoring on the network. The Dual Trunk E1 Router is capable of monitoring up to 16 protocols at a time. The default configuration includes the following protocols:

- IP
- ICMP
- UDP
- TCP
- FTP Control
- FTP Data
- Telnet
- SMTP (e-mail)
- DNS
- HTTP
- NETBIOS Name Service
- NETBIOS Datagram Service
- NETBIOS Session Service
- SNMP

- SNMP Trap
- Lotus Notes

The Dual Trunk E1 Router uses the limited extensibility feature as defined in RFC 2021.

- The protocol directory can process up to 16 protocols
- Each protocol must be a “child protocol” of IP, UDP, or TCP

Using the limited extensibility feature, you can monitor any protocol that rides directly on top of IP, UDP or TCP. You may define a particular value to be recognized in the demultiplexing field of the parent protocol.

NOTE: Changes will be stored in volatile memory and not remembered after the unit has been reset or powered off.

Protocol Distribution

The Protocol Distribution group allows the Dual Trunk E1 Router to discern how much traffic is being used by a specific protocol. When viewing this data in Choice View, you will be able to determine which protocols are the biggest users of the network’s bandwidth. This feature is referred to as Application Top Talkers.

Network Layer and Application Layer Host Tables

RMON-2 allows you to discern which IP addresses are contributing the most traffic to your network, and further, to drill down and find out which applications on these addresses are generating the most activity. Identifying these Top Talkers gives you increased control over your network and bandwidth usage.

The Network Layer Host Table (nlHostTable) provides information on the 256 busiest IP addresses, while the Application Layer Host Table (alHostTable) lists how much traffic a particular IP address is sending using a particular protocol. When an IP address has been identified as one of the Top Talkers, periodically reading the alHostTable with Choice View, will reveal which application on that IP address is using the most bandwidth.

The table has been implemented so that:

- There is one hlHostControlTable entry configured at boot time. Only one entry can exist at a time. It can be set to monitor the entire E1 (default).
- The hlHostControlNIMaxDesiredEntries is set to 256. The Dual Trunk E1 Router builds a table to monitor the activity of 256 IP addresses .
- The hlHostControlAIMaxDesiredEntries is set to 16. You can monitor 16 protocols at a time.

NOTE: If more than 256 IP addresses are detected on the network, the Dual Trunk E1 Router replaces the least seen entry with the new entry in the nlHostTable.

Network Layer and Application LayerMatrix Tables

Through the implementation of standardizedRMON2 network-layer matrix (nlMatrix) and application-layer matrix (alMatrix) groups, the Dual Trunk E1 Router tracks and reports traffic sent between pairs of network addresses and categorizes them by applications and protocols. Standard-based Network Management Software tools, such as Concord Health Traffic Accountant, uses nlMatrix group to generate IP conversation reports, and uses alMatrix to associate the applications involved in the IP conversations. Up to 1024 conversations can be monitored simultaneously.

Optional ChoiceView Plus software application lets you generate IP conversation reports from RMON2 data collected by the Dual Trunk E1 Router.

Alarms

This chapter discusses alarm conditions and how these conditions are displayed.

CONFIGURING ALARM CONDITIONS

When the Dual Trunk E1 Router detects an alarm condition, the unit reports the condition to the terminal.

Depending on your network management environment, the unit may also send alarm messages or SNMP trap messages.

Set alarm conditions in Menu-8A, Alarm Configuration.

The Dual Trunk E1 Router reports alarm conditions to the device connected to its COMM Port (such as a terminal or modem)

SNMP traps are sent as configured in Menu-0B, SNMP Configuration; otherwise, the connection indicated in Menu-8C identifies from where the alarms are reported.

If a modem is connected, the unit causes the modem to dial out (if in Menu 8C, Connection is set to Modem; valid telephone numbers are set in Phone Number 1 or Phone Number 2; in Menu-8A. `Ethernet Signal Loss Alarm` is Enabled and Block all Alarms is set to No).

NOTE: If IP is enabled, only SNMP traps are sent. Alarms will not be displayed on the terminal.

How Alarm Reports Are Displayed

Alarms are displayed on a terminal at the bottom of the screen when the terminal is connected to the COMM Port and you are logged on:
Example—Ethernet Signal Loss Alarm will be given at the bottom of the screen, as follows:

```
??? ID: Oahu Data1 Carrier Loss Start: 07:17:37 Feb.22, 1997--
```

The alarm includes the unit ID, type of alarm, start or end of alarm condition, date, and time. The alarm information remains on the screen either until a new alarm occurs or until you select a new screen.

When no alarm is present, a dotted line (similar in appearance to the one below) is shown:

```
-------------------------------------------
```

When you are not logged on, the alarm appears as a single line showing the unit ID, type of alarm, start or end of alarm, and the time stamp, if IP is disabled.

In SNMP mode, the system sends the alarm as an SNMP trap to the SNMP manager which displays it on the SNMP console.

Menu-8 Alarm

Menu-8, Alarm, provides access to four sub-menus:

- Alarm Configuration
- Miscellaneous Management Configuration
- Modem Initialization Strings
- COMM Port Configuration

Select the corresponding option to view and configure parameters for alarm configuration, external alarm configuration, for miscellaneous management configuration, and modem initialization strings. For more information on Menu 8, see the *4200 WAN Access Platform TUI Reference Guide*.

Menu-8A Alarm Configuration

When you select **Alarm Configuration**, Menu 8A appears. Menu 8A allows you enable or block alarm reporting, and select if alarms associated with the Ethernet signal will be reported.

Menu-8C Miscellaneous Management Configuration

When you select **Miscellaneous Management**, Menu-8C appears. Menu 8C allows you to configure a variety of parameters including connection, phone numbers, timing and error thresholds.

Menu-8E Modem Initialization Strings

If you select **Modem Initialization Strings**, Menu 8E appears Each unit can have a maximum of two modem initialization strings. The first string (`String 1`) can be equal to or less than 20 characters, and the second string (`String 2`) can be equal to or less than 60 characters.

To initiate a modem connection:

1. **The unit sends +++, followed by the first modem initialization string.**
2. **The unit then waits for a response from the modem to guard against the possibility of losing the characters immediately after the modem resets.**
3. **After receiving the modem response, the unit sends the second initialization string (if this string is programmed). The Dual Trunk E1 Router assumes that the modem always sends a response; therefore, *do not* program the modem *not* to send a response.**
4. **If using the modem reset command, you should program everything up to the reset command as the first modem initialization string.**
5. **Program the remaining commands as the second modem initialization string.**

Troubleshooting

Troubleshooting the Unit

This section describes problems you may encounter and provides suggested methods to troubleshoot and resolve the problems.

Unit Problems

A list of possible problems is given in Table 11-1, along with suggested solutions for each.

Table 11-1 Unit Problems *(1 of 4)*

Symptom	Probable Cause	Solution
The LRU4240 does not power up.	• Unit not plugged in. • Loose power connector. • PDU (Power Distributor Unit) isn't powered up/on. • Blown fuse on LRU4240. • Reversed power leads from DC supply (standalone).	• Make sure the unit is plugged into a live AC outlet, if the unit is AC powered. If the shelf is DC powered, make sure the respective DC leads are not crossed. • Check to assure that all fuses are operational; replace as needed. If the problem persists, call Black Box Technical Support for assistance.
The LRU4240 system does not dial out when an alarm occurs.	• Miscellaneous configuration on Alarm Menu-8C. • Modem strings 8E not correct. • Wrong cable. • No modem attached.	• Make sure the connection between the COMM Port and the modem is a crossover (null) modem connection. • A DCE Port is represented the same way as the modem port. • Make sure Connection is set to Modem and two valid telephone numbers are set in Phone Number 1 and Phone Number 2 in Menu-8C. • Make sure Block all Alarms is set to No in Menu-8A and the occurring alarm is set to Enabled. • If the above solutions do not correct the problem, call Black Box Technical Support for assistance.

Table 11-1 Unit Problems *(2 of 4)*

Symptom	Probable Cause	Solution
Current user initiated tests terminate themselves without user intervention.	• Misconfiguration for Menu-9A Timeout.	• Make sure the system is set to run the test for an unlimited amount of time. • Test length options are 15 min., 1 min., 60 min., Unlimited. With Self Test, Loop Up Remote and Loop Down Remote, Unlimited does not apply. • If the above step does not correct the problem, call Black Box Technical Support for assistance.
The system cannot be put into network loopback from the remote unit.	• Unit does not recognize Loop command being sent. • Loopback detect is disabled on unit. • Circuit is down or in Loop towards remote unit.	• Make sure the remote unit is sending the correct loop code. • Make sure the system is set to receive the same standard or alternate code as the remote unit. • Using your E1 test set, send a loop up code into the system. If the system still does not loop up, call Black Box Technical Support for assistance.
The system cannot be put into payload loopback from the network.	• Framing protocol choice. • Wrong timeslots used for test signal.	• Make sure the system is set for T1.403 Annex B fractional loopback code, if the network is sending T1.403 Annex B to loop it up. • Make sure the payload portion you are attempting to loop up has assigned bandwidth. • If the LRU4240 still does not loop up, use your E1 test set to inject a fractional loopback signal into the payload you wish to loop up. • If the above steps fail, call Black Box Technical Support for assistance.
After power-up, the menu clock no longer shows the correct time or date.	• Time not set.	• Set the time in Menu-4. • If the time is still incorrect, call Technical Support.

Table 11-1 Unit Problems *(3 of 4)*

Symptom	Probable Cause	Solution
No response from any unit on the communication network.	• Bad cable. • Wrong baud rate. • Hung terminal. Restart terminal session.	• Make sure that Pin 8, CTS, is not connected at the ASCII terminal end of the COMM Port cable. • Standard Black Box COMM Port cables do not have this connection at the ASCII terminal end. Some ASCII terminals will activate the CTS line, and thus interfere with the LRU4240 collision avoidance. • Get a null modem adapter to cross pins 2 and 3 (transmit and receive) on the terminal. • The COMM Port cable is connected to an inactive or faulty port on the terminal, or the terminal is faulty. • Replace the COMM Port cable if it is faulty. • Make sure the COMM Port parameters match the terminal's parameters.
No response from some units on the network.	• Mismatch baud rate. • Break in cable.	• Make sure the LRU4240 is powered up. • Make sure the unit ID is correct. • Swap the connector positions with a unit that has no problem communicating with the terminal, to find out if a portion of the COMM Port cable is faulty. • Make sure the COMM Port parameters match the terminal's parameters.
Invalid data is received from one or all units on the network.	• Baud rate configuration. • EMI. • Two units with the same ID.	• Make sure the COMM Port parameters (on the problem units) match the terminal's parameters. • Verify that none of the units are missing an ID and that no two units have the same unit ID.

Table 11-1 Unit Problems *(4 of 4)*

Symptom	Probable Cause	Solution
Some invalid data is received mixed in with a mostly good menu display.	• Refresh screen image. • 1 or more units are missing at ID, or two units have the same ID.	• To refresh screen, press **`Ctrl-L.`** • Reduce the baud rate on the units and terminal if you are using the maximum (38400 baud) for communicating with a very large number of units. • If the cable from the network to the terminal exceeds the 15 m (50 ft.) maximum, fix the length. • Verify that none of the units are missing an ID and that no two units have the same unit ID.

NETWORK PROBLEMS

Table 11-2 Network Problems *(1 of 4)*

Symptom	Probable Cause	Solution
The unit experiences a loss of signal or a loss of frame on the Network Port.	• Equipment Failure	• Test E1. • Apply hardware loop to front of unit.

Table 11-2 Network Problems *(2 of 4)*

Symptom	Probable Cause	Solution
The NET LED does not illuminate.	• No incoming signal. • Bad LED.	• Run a lamp test from Menu-9, Diagnostics to make sure the LEDs are working. • Make sure the E1 line from your service provider is connected to the RJ-48C female connector on the back of the LRU4240 NTU. • Remove the E1 line from the back of the LRU4240 and place the E1 test set in its place. Connect the transmit of the E1 test set to the receive of the network plug (pins 3 and 11, 3—tip, 11—ring). If the NET LED changes to any color, i.e., green or red, contact your service provider for assistance with cutting over the E1 line. • Place the E1 loopback plug on the network connector on the back of the LRU4240. If it then changes color, troubleshoot your test setup. • If the NET LED never lights, call Black Box Technical Support for assistance.
The NET LED is constantly red.	• Constant out-of-sync or out-of-frame on E1. • Misframe/FE. • Carrier has problem. • Configuration doesn't match framing.	• Make sure the E1 line framing format matches the LRU4240's framing format. • Check the LRU4240 for excessive errors. • In CRC4-Enabled mode, check for CRC and CV; in CRC4-Disabled mode, check for CVs only. If excessive errors appear, place your E1 test set or your loopback plug on the RJ-48C or BNC socket on the back of the system to see if the errors stop. • If they do, contact your service provider for assistance. • If the errors do not stop, call Black Box Technical Support for assistance.

Table 11-2 Network Problems *(3 of 4)*

Symptom	Probable Cause	Solution
The NET LED remains constant amber/yellow.	• Incoming RAI or UAI.	• Check to see if the LRU4240 is receiving a RAI alarm or an AIS alarm. • Make sure the remote/far end system is receiving a proper E1 signal. If it is not, it will be generating a RAI alarm towards your equipment. • If the system is still receiving a RAI alarm, place the E1 test set or the E1 loopback plug on the RJ-48C or BNC socket on the back of the LRU4240. If the RAI alarm stops, contact your service provider for assistance. • If, after all above steps have been satisfied, your LRU4240 still shows a yellow **NET** LED, call Black Box Technical Support for assistance.

Table 11-2 Network Problems *(4 of 4)*

Symptom	Probable Cause	Solution
The NET LED flickers intermittently between red, amber and green.	• Receiving errors on NET Port (CV, CRC, FE, etc).	• Make sure the timing source is properly configured. Timing should be set to NETWORK if the network is the source. • If it is not the source, timing should be set to INTERNAL at one E1 end, and NETWORK at the other end. • If you're not sure that the network is the source, contact the network provider and discuss your circuit order. The provider will tell you if the E1 network is the source. • If the timing source is properly configured and the NET LED continues to flicker between red, amber and green, isolate the system with the E1 test set to see if the problem clears. • Place the E1 test set into the proper timing mode (provide timing or recover timing). You cannot use the loopback plug in this application since it would require us to provide timing and would not allow us to see if we can recover timing from a valid E1 source. • If the NET LED continues to flicker, call Black Box Technical Support for assistance.

Specifications

TECHNICAL SPECIFICATIONS

Performance

Item	Rating
Maximum Packet Length	• 65535 bytes (for payload traffic) • 1536 bytes (for SNMP management)
Maximum Packet Rate	11,000 packets/sec duplex. Dual Trunk E1 Router will discard packets over this amount

LRU4240 Network Interface

Item	Rating
Transmit bit rate	2.048 Mbs ± 50 ppm
Receive bit rate	2.048 Mbs ± 75 ppm
Line code	HDB3
Framing	ITU-TS G.704/CTR 12
Pulse shape	ITU-TS G.703/CTR 12
Jitter	ITU-TS G.823/CTR 12
Output level	ITU-TS G.703/CTR 12
System timing	Network 1, Network2 , or Internal
Input level	0 to -26 dB
Impedance	75 Ohm (BNC) unbalanced or 120 Ohm (RJ-48) balanced

LRU4240 Data Interface

Item	Specification
Interface types	Ethernet 10BaseT

Power Options

Item	Specification
AC Power	Universal Power Supply 100 VAC to 240 VAC Autoranging, 50/60 Hz
DC Power	-40 VDC to -78 VDC Through two-position Phoenix connector
Power Consumption	9 W maximum per unit

Physical

Item	Specification
Dimensions	8.75 in W (22.2 cm) x 1.75 in H (4.4 cm) x 12 in depth (30.4 cm)
Weight	6.5 lb (3.0 kg)
Network Connector	RJ-48
COMM Port Connector	8 Pin modular
Ethernet Management Interface	RJ-45 socket

Environmental

Item	Specification
Operating Temperature	0°C to 50°C (32°F to 122°F) ambient
Storage Temperature	-20°C to +60°C (-4°F to 140°F)
Relative Humidity	0% to 95% noncondensing
Altitude	15,000 ft (4.6 km)

Reliability

MTBF 12 years minimum

LRU4240 Diagnostics

Item	Diagnostics And Tests
Loopbacks	E1 Network, E1 Payload, Fractional E1 Payload
E1 Loopback Control	Set/Reset Code, Front Panel, COMM Port
Fractional Payload	
Loopback Control	CCITT V.54 Sequence, COMM Port

Item	Diagnostics And Tests
Test Patterns	QRW, 1:1, 1:7, 3:24, All 1s, All 0s, 2-User Programmable 24 Bit Patterns, bit error injection
Alarm Parameters	
E1 Network Port	NET Carrier Loss Alarm
	NET Sync Loss Alarm
	NET AIS Alarm
	NET RAI Alarm
	CRC, CV, FE Threshold Alarm

Dual Trunk E1 Router

Table A-1 Default Configuration *(1 of 2)*

Configuration	Factory Default Settings	Your Configuration
Unit Configuration		
Unit ID	Unique ID assigned	
Protect Mode	Disabled	
Idle Code	0xFF	
In-band Monitoring	Enabled	
Link Monitored	Net 1 (in independent links)	
	Net (in MLPPP mode)	
Network port 1 Configuration		
CRC4		
Main Sync Source	Enabled	
Alternate Sync Source	Network	
	Internal	
Network port 2 (Aux) Configuration		
CRC4	Enabled	
Main Sync Source	Network	
Alternate Sync Source	Internal	
Diagnostic Configuration		
User Pattern 1	00110011001100110011001100110011	
User Pattern 2	00000001000000010000000100000001	
Alarm Configuration		
Block All Alarms	Disabled	
Net Carrier Loss Alarm	Enabled	
Net UAI received Alarm	Enabled	
Net RAI received Alarm	Enabled	
Loss of Signal from data port	Enabled	
Net Sync Loss Alarm	Disabled	
CV Threshold Alarm	Disabled	
CRC Threshold Alarm	Disabled	
Ethernet loss signal Alarm	Enabled	
FE Threshold Alarm	Disabled	
SNMP Configuration		
1st NMS Address	0.0.0.0	
1st Output Port	COM	
2nd NMS Address	0.0.0.0	
2nd Output Port	COM	
3rd NMS Address	0.0.0.0	
3rd Output Port	COM	
Get Community String	public	
Set Community String	public	
Trap Community String	public	

Table A-1 Default Configuration *(2 of 2)*

Configuration	Factory Default Settings	Your Configuration
COMM Port and Terminal Configuration	Direct	
Connection	10 minutes	
Timeout when Logged on	Unlimited	
Timeout when not Logged on	38400, 8, no parity, 2 stop bits	
COMM Port	Enabled	
Terminal Mode	Not Assigned	
Phone Number 1	Not Assigned	
Phone Number 2	Not Assigned	
Normal User Password	Not Assigned	
Superuser Password	Not Assigned	
Modem String Configuration		
Modem String 1	ATEOVOZO	
Modem String 2	ATV0E0Q0F1C1S0=1S2=43S3=13S4=10S7=30S12=50&C1&D0	
Ethernet Configuration		
IP Address	0.0.0.0	
IP Mask	0.0.0.0	
IP Gateway	0.0.0.0	
MAC Address	(Unique ID assigned)	

Dual Trunk E1 Router

Cable and Connector Pin Assignments

E1 Network Pin Assignments

The pin assignments for the RJ48 network interface connector are listed in the Table B-1 below.

Table B-1 Network Interface Pin Assignments

RJ48 Pin	Signal
5	Send toward Network Tip (T1)
4	Send toward Network Ring (R1)
2	Receive from Network Tip (T)
1	Receive from Network Ring (R)
3, 6, 7, 8	NC

COMMUNICATION PORT PIN ASSIGNMENTS

Table B-7 describes the COMM Port (RJ45) pin assignments.

Table B-2 Communication Port Pin Assignments

RJ45 Pins	Signal	Description
3	SD	Send Data (from Dual Trunk E1 Router to terminal)
6	RD	Receive Data (from terminal to Dual Trunk E1 Router)
8[1]	CTS	Clear To Send (I/O to all Dual Trunk E1 Routers only)
4, 5	SG	Signal Ground (bi-directional)
7	DCD	Carrier Detect

1. CTS is used by the Dual Trunk E1 Router as a collision avoidance line. This line should not be connected at the CRT terminal end of the COMM Port cable.

DE-9 to DB-25 Adapter Pin Assignments

BlackBox can provide a DE-9 to DB-25 adapter for the BlackBox DE-9 COMM Port ribbon cable. The pinout assignments for the adapter are listed in Table B-8 below.

Table B-3 DE-9 to DB-25 Adapter Pinouts

DE-9	DB-25
3	2
2	3
7	4
8	5
6	6
5	7
1	8
9	23
4	21

Software Upgrade

SOFTWARE DOWNLOAD

The Download feature enables you to upgrade software, and includes the following capabilities:

- Separates the downloading operation from switching to new software, where these operations can be performed at separate times. You can schedule a time at which the unit can be initialized with the new code.
- Command remotely using SNMP the TFTP/XModem download and code switching
- The unit stores two images of executable code; you can switch between the two images.
- Enables downloading of the new software while the unit is operational and passing data. The code can be downloaded through:
    - Xmodem via the terminal user interface using an asynchronous connection.
    - TFTP from a network management station to the unit via SLIP using an asynchronous connection or through NET or Ethernet Ports in-band.
    - TFTP via Ethernet.

Using the Download Menu Utility

Use the Download Utility menu, accessed through Menu-4, Main Configuration, to download software updates. You may use the Xmodem protocol or TFTP. When switching from one executable image to another, the operational software in the unit is restarted, which results in a temporary service interruption lasting from one to two minutes.

During the download sequence, the Power/Test LED will blink alternating red and green.

Setting Up for Xmodem

To download new software:

1. **Insert the new software diskette in the drive of the PC.**
2. **From Menu-4 Main Configuration, type F (as instructed in the menu for FLASH Download) to start the download session.**
3. **Menu 4F (Software Download Menu) will appear**
4. **Select the Protocol (Xmodem or TFTP) to Xmodem under `Protocol`.**
5. **Press A to start the download.**

Setting Up for TFTP

Use these steps to set up for TFTP::

1. **Set the download protocol in the Download utility to TFTP.**

2. **Press A in the Download Utility menu.**

3. **Start TFTP for the Network Management System, and indicate binary mode.**

Abnormal Termination

The following list summarizes scenarios during which the downloading process may fail:

- Software load is corrupted.
- Transmission errors.
- Failure of the downloading computer, the modem (if one is used), the connection between the downloading computer and the unit or a failure of the unit, which also includes a power failure.
- User aborted the download process.
- Time-out built into the Xmodem or TFTP protocols.

Typically, abnormal termination of the download process leaves the Code File in a non-usable state. In this case, the Download Utility will indicate that the Code File is unavailable.

Error Indicators

If the download utility fails, an error indicator appears in the Download Utility menu. Depending on the error indicator listed below in Table C-1, you can take the following action or at least be apprised of the condition:

Table C-1 Download Utility Error Indicators *(1 of 2)*

Error Type	Error Indicator	Description (Message)
General	1	Software error. Note the specific error information, and call Black Box Technical Support.
	2	Load Received is corrupted.
	3	Load Received has invalid embedded length.
	4	Load Received is invalid for this unit.
Hardware	5	Flash-ROM Not Supported.
	6	Flash-ROM With Protected Sector.
	7	Flash-ROM Failed To Erase.
	8	Flash-ROM Failed To Program.
Xmodem	9	Xmodem Abort Received.
	10	Xmodem Data Timeout.
	11	Xmodem Invalid Sequence.
	12	Xmodem Unexpected Data.
	13	Xmodem Packet Timeout.
	14	Xmodem Packet Corrupted.
	15	Xmodem Failed to Acknowledge.

Table C-1 Download Utility Error Indicators *(2 of 2)*

Error Type	Error Indicator	Description (Message)
	16	Xmodem Reserved.
	17	Xmodem Reserved.
	18	Xmodem Reserved.
TFTP	19	TFTP Error Packet Received
	20	TFTP Invalid Mode.
	21	TFTP Invalid Opcode.
	22	TFTP Unexpected Opcode Sequence.
	23	TFTP Invalid Packet Length.
	24	TFTP Invalid Data Packet Sequence.
	25	TFTP Request Timeout.
	26	TFTP Data Packet Timeout.
	27	TFTP Failed to Acknowledge.

Download Aborted by User

You may abort the Xmodem downloading process by pressing **`Ctrl-x`**.

To perform the downloading abort, instruct the terminal emulator program to abort the Xmodem download process and return to terminal mode. The specific procedure depends on the terminal emulator program being used. The recovery is the same as explained under Abnormal Termination.

With TFTP, the procedure to discontinue the TFTP session depends on the TFTP setup. Again, the recovery is the same as explained under Abnormal Termination.

The parameter groups for the Download Utility are given in Table 11-3.

Table 11-3 Menu 4F Download Utility *(1 of 2)*

Group	Field	Description
CODE FILE	1 Version	Version of the operational software residing in Code-File 1. This field reads “Absent” if there is no operational software stored in this code-file or if the operational software is corrupted.
	2 Version	Version of the operational software residing in Code-File 2. This field reads “Absent” if there is no operational software stored in this code-file or if the operational software is corrupted.

Table 11-3 Menu 4F Download Utility *(2 of 2)*

Group	Field	Description
DOWNLOAD	Code File	The Code-File that will receive the downloaded operational-code, and that is currently not operational.
	Status	Shows the status of the download, and is either Idle, Start, In Progress, Verifying, Success, or error. This field is updated after an Xmodem download to the local unit. If the status is "Error", then a number associated with the failure indicates the specific problem.
	Error	Indicates a specific problem during download.
	Bytes Received	Shows the number of bytes received during the download. This field is updated after an Xmodem download to the local unit.
	Protocol	Protocol used for the download. Choices are Xmodem and TFTP.
CHANGE	Code File	Code-File to be switched over when the scheduled time is reached. Choices are NONE, 1, and 2. NONE indicates that no change is desired, and can be used to cancel a scheduled change.
	Method	Either SCHEDULED or NOW. NOW indicates that the change occurs immediately, and SCHEDULED indicates that the change occurs when the actual time reaches the scheduled time.
	Scheduled Date	Expressed in DD/MM/YY (day, month, and year) at which the switch-over will occur.
	Scheduled Time	Expressed in HH:MM:SS (hours, minutes, seconds) at which the switch-over will occur.
	Count Down	Shows the time interval HH:MM:SS (hours, minutes, seconds) for the switch-over to occur after it has been initiated. If the switch-over has not been initiated, then it shows "Press 2 To Start" or "Press 4 To Start" for the local unit and the remote unit, respectively.

Programming software upgrades remotely

Starting with software release 2.3RT, you can initiate the code download and initialization remotely using SNMP commands. The Menu-4 download utility commands, download method (TFTP or Xmodem) and schedule date and time, have associated SNMP variables in the eclipse MIB.

The sample script shown below illustrates a remote TFTP download:

```
#!/bin/ksh
NODE="172.25.150.1"
BIN_FILE="074-04240-01sr2.3RT.bin"

 snmpset  $NODE  .1.3.6.1.4.1.300.200.2.49.1.0 integer 1
 tftp $NODE <<EOT
 bin
 put $BIN_FILE
 quit
```

```
EOT
  snmpget 172.25.150.1 .1.3.6.1.4.1.300.200.2.49.5
  snmpget 172.25.150.1 .1.3.6.1.4.1.300.200.2.49.9
```

SOFTWARE-ONLY UPGRADES

All upgrades to the 4200 WAN Access Platform are software-only upgrades. The hardware unit ships from the factory with all the physical ports even if they are not used with the configured software. The physical ports include two serial DTE ports, two T1/E1 ports, COMM port, and Ethernet port.

Changing software

You can also change the software configuration of your 4200T/E . For example you can reconfigure your unit from a 4210 CSU/DSU to a 4230 Access Router. This configuration change requires downloading a new software code into the unit, configuring the software menus, and changing the network and DTE connections.

Contact BlackBox Technical support to obtain any software upgrade.

Menus

This appendix lists all of the Dual Trunk E1 Router Menus and their descriptions.

Table D-1 Router Menus *(1 of 5)*

Menu Number	Name	Description	Page
0	IP Configuration	Selection menu for following submenus: • Interface configuration • SNMP configuration • Ethernet configuration • Performance monitoring configuration • LMI configuration • SLA configuration	113
0A	Interface Configuration	Traffic type (PPP or Frame Relay), Multilink, Interface IP addresses (Ethernet, Network, and COMM ports).	113
0B	SNMP Configuration	SNMP Traps, NMS IP addresses andcommunications Settings.	114
0C	Ethernet Configuration	Configure data speed mode (Full or half duplex).	115
0E	Performance monitoring	Frame Relay performance monitoring.	115
0F	LMI configuration	Enable LMI and set polling and error parameters. Set UNI-U or UNI-N interfaces.	116
0H	SLA configuration	Frame Relay SLA FRF.13 configuration	116
0L	Outage source configuration	Reserved. Do not use.	
1	Main Status	Displays unit status, LAN and WAN connection status (Ethernet, NET1, and NET2.	117
2	Ethernet Data Status	Shows the status of the ethernet port. “Link up” or “Link Down”.	None
3	Reports	Access to carriers and users registers reports, inband reports, SLA reports, Ethernet and IP statistics.	
3A	Carrier Reports	Carrier Reports lets you access network ports physical layer statistics. Select which of the NET1, NET2, or aggregate carrier registers to display. Use n (for next) and p (for previous) to select which of the three network ports (NET1, NET2, or aggregate) you want to view statistics.	118
	3AA- Carrier Registers, Current Interval	Real-time statistics for current interval.	118
	3AB- Carrier Registers, Total Over 24 Hours	Net statistics in for last 24 hours. Summary.	118
	3AC- Carrier Registers, 24 Hour Detail	Net statistics for last 24 hours in 15-minute intervals.	118
	3AE- Carrier Registers, 4 Day Detail	Net statistics in 384 15-minute intervals.	118

Table D-1 Router Menus *(2 of 5)*

Menu Number	Name	Description	Page
	3AF- Carrier Registers, 14 Day Summary	Net statistics for last 14 days. Summary.	118
	3AG- Carrier Registers, uptime total	Net statistics for uptime interval.	118
3B	User Reports	User Reports submenu.	118
	3BA- User Registers, Current Interval	Net statistics for the current interval	118
	3BB- User Registers, 24 Hour Total	Net statistics for last 24 hours. Summary.	118
	3BC- User Registers, 24 Hour Detail	Net statistics in 96 15-minute intervals.	118
	3BE- User Registers, 4 Day Detail	Net statistics in 384 15-minute intervals.	118
	3BF- User Registers, 14 Day Summary	Net statistics for last 14 days. Summary.	118
	3BG- User Registers, uptime total	Net statistics for uptime interval. Summary.	118
3C	In-band Reports	Inband Reports submenu.	119
	3CA- In-band Ethernet Registers, current interval	Provides detail inband Ethernet Registers for the current 15 minutes interval.	119
	3CB- Inband Network Registers, current intervall	Provides detail on inband network registers for the current 15 minutes interval.	119
	3CC- Inband Ethernet registers, 24 Hour total	Shows inband Ethernet registers in 96 fifteen-minute intervals.	119
	3CE- Inband Network registers, 24 Hour tota	Displays inband network registers in last 96 fifteen minutes	119
	3CF- Inband Ethernet registers, lifetime total	Displays inband ethernet registers lifetime counters.	119
	3CG- Inband Network registers, lifetime total	Displays inband network registers lifetime counters.	119
	3CH- Inband Ethernet registers, 24 hour details	Inband Ethernet registers performance data for the last 24 hours.	119
	3CI- Inband Network registers, 24 hour detail	Inband Network registers performance data for the last 24 hour detail	119
3E	PPP statistics	Displays the PPP Link Control Protocol (LCP) and Network Control Protocol (LCP) statistics enabling you to troubleshoot PPP and MLPPP sessions.	

Table D-1 Router Menus *(3 of 5)*

Menu Number	Name	Description	Page
3E	In Frame Relay mode: SLA Reports	Displays the SLA reports submenu	
3EA	DLCI Outages	Provides information on the type, number, and duration of outages on a per DLCI basis. As specified in FRF.13, outages are defined as either Fault (Outages) or Excluded.	119
3EB	Frame Transfer Delays	Provides information on the number of threshold violations per DLCI.	120
3EC	Local Transmit Data Delivery Report	Provides information on the network's (per DLCI) effectiveness in transporting data. It also provides the DDR for data delivered within CIR, and data delivered in excess of CIR.	120
3EE	Local Receive Data Delivery Report	Provides information on the network's (per DLCI) effectiveness in receiving data. It also provides the DDR for data received within CIR, and data received in excess of CIR.	120
3EF	Local Transmit Frame Delivery Report	Provides a view of how effective the frame relay network has been effective at packet transmission.	121
3EG	Local Receive Frame Delivery Report	Provides a view of how effective the network has been at packet reception.	121
3FA	Ethernet physical layer	Displays the ethernet protocol statistics which includes FCS errors, total single collision frames, total number of deferred transmissions, total number of late collisions, total number of carrier sense errors, and total number of frames received that are too long.	121
3FB	Ethernet interface statistics	Displays data ethernet statistics which include totals for octets received/transmitted, unicast packets received/transmitted, non unicast packets received/transmitted, number of packets received with unknown protocol IDs, RX packets received with Ethernet errors, and non-routable RX packets received.	121
3FC	IP statistics	Displays IP MIB statistics including: totals packets received	122
3FE	ICMP receive statistics	Displays performance data for every 15-minute interval in the last 4 days. (up to 32 screens)	122
3FF	ICMP tranmist statistics	Displays performance data totals for each day, for the last 14 days	123
3FG	ARP statistics	Displays performance data uptime totals for the NET1, NET2, and aggregate network por	123
3M	Delay monitoring results	Displays results of "Delay Monitoring configuration" tests initiated from menu-9C	123
3Z	Event Log	Alarm History log.	124
4A	Unit Configuration	Set general configuration parameters.	126
4B	Net Configuration and Status	View status of individual links and choose line setting for each port.	126
4F	Download Utility Screen	See "Software Download" on page 103	
4T	GMT Time sync	Configure time and date synchronization (RFC868).	page 126

Table D-1 Router Menus *(4 of 5)*

Menu Number	Name	Description	Page
4V	Timezone configuration	Set unit's local time. This menu works in conjunction with GMT Time Sync menu-4T (RFC-868). When RFC 868 is used to get time, time server provides GMT. If a unit is deployed in different time zone user needs to configure the units appropriately.Day light savings ends in October.	127
6A	MLFR Configuration	View and set the following Multilink Frame Relay configuration parameters: Link Integrity Timer, Link Acknowledge, and Retry Counter.	127
6A	PPP/MLPPP Unit configuration	View and set PPP configuration parameters.	127
6B	MFR port configuration	View link status and protocol errors per link.	128
6B	PPP/MLPPP Port Status	View link status and protocol errors per link.	127
6Z	Timeslot Configuration	Fractional E1 speed configuration and port mapping to Ethernet data port.	
7	Features	Reserved for software feature key upgrades.	128
8	Alarm	Alarm Selection submenu.	
8A	Alarm Configuration	Allows user to enable/disable alarms and to set alarm thresholds.	128
8C	Miscellaneous Management Configuration	Dial out, passwords, alarm port settings.	129
8E	Modem Initialization Strings	Setting menu for modem initialization strings.	130
8F	Comm port configuration	Configure the comm port speed	130
8G	User authentication server	Configure Radius authentication protocol. See “Configuring Radius Authentication” on page 36	36
8O	Reboot the unit	Rebooting the unit remotely using TUI menu	
9	Diagnostics	Tests and diagnostics selection menu.	
9A	Physical Layer Diagnostics	E1 Net testing by patterns, loop, selecting loop codes on/off.	130
9B	Link Layer Diagnostics	Menu for In-band testing.	132
9C	Delay Monitoring Configuration	Configuration for Delay Monitoring. Results are displayed in Menu-3M.	133
$	Routing Configuration	Main router configuration menu	
$A	Unit Routing configuration	Configuration routing mode, default gateway IP address, enable Firewall, and Load balancing.	133
$B	Display routing table	View routing configuration tables (static and dynamic routes)	134
$C	Static routing table	Configure static routes.	134
$E	Routing Command Line Interface (CLI)	Allows you to configure the dynamic routing protocols (RIP1, RIP2, and OSPF) See “Kernel Command Reference” on page 164.	
$F	Display ARP Table	View ARP cache table.	134
$H	Firewall Table	Configure access lists.	134

Table D-1 Router Menus *(5 of 5)*

Menu Number	Name	Description	Page
$IA	Static Frame Relay Map config	Configure manually DLCI to IP address mappings. See "Configuring Frame Relay DLCIs" on page 33	
$IB	Display active Frame Relay Map Table	View current DLCI to IP address mappings. If inverse ARP is enabled on an interface, DLCI to IP address mappings is automatically learnt. Manually configured mappings are also displayed on this menu.	
$JA	NAP/NAPT configuration - Global Map table	Configure global IP addresses and mapping to network interfaces. See "Configuring NAT" on page 54	
$JB	NAP/NAPT configuration - Static table	Assign manually global IP addresses to local hosts. See "Configuring NAT" on page 54	
$JC	NAP/NAPT configuration - Local address table	Configure local networks requiring NAT. "NAT Configuration menus" on page 54	
$JE	NAT Configuration	Enable or disable unit NAT configuration. Enable/Disable NAT, overloading (NAPT) per network interface.	
$JF	NAT Dynamic entries	Displays current global IP addresses allocated through NAT.	
$K	DHCP configuration	Enable/Disable DHCP relay and configure DHCP relay server IP address	135

Table D-2 Menu-0A - Interface configuration

Parameter	Parameter—Options ; Definition
UNIT	**In-band monitoring** Enables or disables in-band monitoring.
	Traffic Type Set WAN protocol to PPP or Frame Relay. The selected WAN protocol applies to all WAN interfaces. In PPP mode all the TUI menus will be configured for PPP operations. In Frame Relay mode all the TUI menus will be configured for Frame Relay or Multilink Frame Relay operations.
	Multilink Protocol • Select Yes to enable multilink PPP (MLPPP) or multilink Frame Relay (MFR) according to the selected traffic type set above. Both T1/E1 links will be bonded as a single virtual connection and will be identified as **bundle0**. • Select No to enable independent E1 links. The two E1 links will be identified as NET1 and NET2.
COMM	**IP Address** Set the COMM port IP Address in standard IP form (nnn.nnn.nnn.nnn). **Len** Set the IP mask

Parameter	Parameter—Options ; Definition
ENET	**IP Address/Len** Set the Ethernet port IP Address in standard IP form (nnn.nnn.nnn.nnn). **Len** Set the subnet *mask* (1 to 32) which is the part of the IP address shared by all devices on the same network **ICMP Redirect** Enable or disable sending ICMP Redirect message on ENET interface
NET1	**IP Address/Len** Set the first network port IP address that is responded to for in-band traffic received from the NET1, in standard IP form (nnn.nnn.nnn.nnn). **Len** Set the IP mask
NET2	**IP Address/Len** Set the second network IP address that is responded to for in-band traffic received from the NET2, in standard IP form (nnn.nnn.nnn.nnn). **Len** Set the IP mask

Table D-3 Menu-0B SNMP Configuration

Parameter	Description
COMMUNITY Get	Enter an alphanumeric text string (max—32 characters). The router SNMP agent uses this text string to check GET requests for the SNMP configuration from the SNMP management station. Default: public
COMMUNITY Set	Enter an alphanumeric text string (max—32 characters). The router SNMP agent uses this text string to check SET requests from the SNMP management station to set the SNMP configuration. Default: public
COMMUNITY Trap	Enter an alphanumeric text string (max—32 characters) which the router SNMP agent inserts in SNMP traps it sends to the SNMP management stations Default: public
TRAP 1st NMS IP Address	Enter the IP address of the first Network Management Server. The router sends trap messages to this server. Default: 0.0.0.0
TRAP 2nd NMS IP Address	Enter the IP address of the second Network Management Server. The router sends trap messages to this server.
TRAP 3rd NMS IP Address	Enter the IP address of the third Network Management Server. The router sends trap messages to this server. Note: If all three trap NMS IP addresses are set, the router sends a trap to all three network management servers.
TRAP 1st Output Port	COMM, ENET, NET Selects the DLCI (if applicable) and port over which the router will send a trap to the 1st NMS IP address.

Table D-3 Menu-0B SNMP Configuration

Parameter	Description
TRAP 2nd Output Port	COMM, ENET, NET Selects the DLCI (if applicable) and port over which the router will send a trap to the 2nd NMS IP address.
TRAP 3rd Output Port	COMM, ENET, NET Selects the DLCI (if applicable) and port over which the router will send a trap to the 2nd NMS IP address.

Table D-4 Menu-0C Ethernet Configuration

Parameter	Description
MAC Address	Read-only Ethernet port MAC address assigned at factory.
Data speed mode	Ethernet port speed 10MB/Half (default) or 10MB/Full
ProxyARP	Reserved for IP Fast Forwarding mode. This feature is no longer supported. Enable or disable ProxyARP in Fast forwarding mode. Default is disabled.
Net directed broadcast mode	Reserved for IP Fast Forwarding mode. This feature is no longer supported. Configurable option available in Fast Forwarding mode only. Enter the network directed broadcast IP address mask
Fwd Multicast	Reserved for IP Fast Forwarding mode. This feature is no longer supported. Configurable option available in Fast Forwarding mode only. Enable or disable forwarding mulcast packets.

Table D-5 Menu-0E Performance Monitoring Configuration

Parameter	Parameter - Options; Definition
Interface	The network interface (NET1, NET2, or NET) to which the DLCI is attached
DLCI	DLCIs will be autodiscovered if LMI is enabled on menu-0F. If LMI is not enabled, the DLCIs must be entered manually on this table. To change a DLCI status to Deleted, enter a zero for the DLCI number. If LMI is enabled, and the DLCI still exists, it will be discovered again and its status returned toa active. Default: 0
CIR	The Committed information rate. If LMI revision 1 is being used, this will be discovered; otherwise, you will need to enter the CIR for each DLCI Default: 0
Delay Threshold	The range is 0 to 64000 milliseconds. When the round trip delay over the PVC exceeds this value: • An event will be registered in the Event Log • A trap will be sent to the NMS (if configured) • An alarm message will be displayed on the terminal user interface • A delay threshold violation is counted

Table D-5 Menu-0E Performance Monitoring Configuration

Parameter	Parameter - Options; Definition
Status	Active - Passing data through the Permanent Virtual Circuit (PVC) Inactive - PVC is broken Deleted - PVC is not available

Table D-6 Menu-0F LMI Configuration

Parameter	Parameter- Options; Definition
Enable	Enable or disable LMI
Type	Select between Annex A, Annex D, and LMI revision 1. Default: Annex D
Enquiry Tx Timer	Sets the interval between STATUS ENQUIRY messages. Set the value between 5 and 30 seconds, in increments of 5. Default: 10 seconds
Full status count	Sets the number of polling cycles for Link Verification before the unit generates the Full Status request. Set the count to an integer between 1 and 255
Max Lmi Error	The number of errors that can occur on the LMI link before the reporting that the interface is down.
Enquiry Rx Timer	Sets the number of seconds between the sending of a STATUS ENQUIRY and the reception of the response. Set this value to an integer between 5 and 30, in increments of 5. Default: 15 seconds
Unit Location	Select UNI-U or UNI-N.

Table D-7 Menu-0H SLA Configuration

Parameter	Description
Enable -	Set this field to Enabled to collect SLA data **Default:** Disabled
FDR/DDR Sample Period	Set the sampling period between 1 minute and 255 minutes. The time period represents the time interval between requests to the far end of the PVC. **Default:** 1
FDR Threshold	Set this threshold between 0% and 100%. 0% means this feature is disabled. Configurable to one thousandth of a percent (for example, 99.999%). When the FDR falls below this threshold: • An event is sent to the Event Log • A trap will be sent to the NMS (if configured) • An alarm message will be displayed on the Terminal User Interface • An FDR threshold violation is counted0% **Default:** 0%

Table D-7 Menu-0H SLA Configuration

Parameter	Description
DDR Threshold	Set this threshold between 0% and 100%. 0% means that this feature is disabled. Configurable to one thousandth of a percent (for example, 99.999%). When the DDR falls below this threshold: • An event is sent to the Event Log • A trap will be sent to the NMS (if configured) • An alarm message will be displayed on the Terminal User Interface • A DDR threshold violation is counted0% **Default:** 0%
Delay Period	Set the Delay Period between 1 minute and 255 minutes. This figure represents the time interval between delay measurements on each PVC. **Default:** 1
Delay Packet Size	Set the Delay Packet Size between 50 bytes and 1500 bytes. This figure represents the size of Request and REsponse packets used to measure delay. **Default:** 128

Table D-8 Main-1 Status

Parameter	Description
Unit status	Indicates the Dual Trunk E1 Router is operating normally, or if any special conditions exist.
Network status	Displays information on the condition of the received T1 or E1 signal.
Ethernet status	Indicates if the Ethernet link is up or down.
Link1/Link 2 status	Indicates the status, up or down, of the network link 1(NET1) and network link 2 (NET2).

Table D-9 Menu-1 Unit Status *(1 of 2)*

Indication	Description
Normal	No abnormal conditions exist.
Self Test	Unit is running self test.
Net Lpbk (port)	Unit is in network loopback.
PLD Lpbk (port, fraction)	Unit is in payload loopback.
Send User 1 (port, fraction) port = Net1 or Net2	Unit is sending User 1 pattern.
Send User 2 (port, fraction)	Unit is sending User 2 pattern.
Send 1:1 (port, fraction)	Unit is sending alternate 1s and 0s.
Send 1:2 (port, fraction)	Unit is sending standard loopdown remote code continuously.
Send 1:4 (port, fraction)	Unit is sending standard loopup remote code continuously.
Send 1:7 (port, fraction)	Unit is sending 1:7 pattern.
Send 3:24 (port, fraction)	Unit is sending 3:24 pattern.

Table D-9 Menu-1 Unit Status *(2 of 2)*

Indication	Description
Send QRW (port, fraction)	Unit is sending QRW code.
Send All 1s (port, fraction)	Unit is sending all ones signal.
Send all 0s (port, fraction)	Unit is sending all zeros signal.
LP UP Remote (port, fraction)	Unit is sending loopdown code to remote site for 15 seconds.
LP DN Remote (port, fraction)	Unit is sending loopup code to remote site for 15 seconds.
No clock	Main clock source has failed.
Lamp Test	Unit is undergoing Lamp Test.

Table D-10 Menu-1 Network Status

Indication	Description
Normal Operation	No abnormal conditions exist.
Loss of Signal	Network signal is missing.
Loss of Frame	Network frame is missing.
AIS Alarm Received	AIS/keep alive.
RAI Alarm Received	Unit has received RAI
Set Code Received	Unit has received set code.
Reset Code Received	Unit has received reset code.
Excessive CRC Errors	Unit has exceeded BPV threshold.
Excessive OOF Errors	Unit has exceeded OOF threshold.

Table D-11 Menu-3A Carrier Reports and 3B User Reports

Event	Default
Unavailable Signal State - In ESF mode, this state is declared at the onset of ten consecutive SESs.	No
Current Interval Timer - Displays the amount to time in a current interval, 0 - 899 seconds.	0
Errored Seconds (ES) - In ESF framing, a second with one or more ESF frame errors or CRC-6 errors.	0
Unavailable Seconds (UAS) - In ESF mode, the number of seconds elapsed after 10 consecutive SES events are received.	0
Severely Errored Seconds (SES) - In ESF mode, a second during which 320 or more CRC-6 violations or OOF events have occurred.	0
Bursty Errored Seconds (BES) - In ESF mode, a second with two CRC-6 errors to 320 CRC-6 errors.	0
Background Block Error (BBE) -	

Table D-11 Menu-3A Carrier Reports and 3B User Reports

Event	Default
Loss of Frame Count (LOFC) - In ESF mode, the number of times Loss of Frame is detected.	0
Controlled Slip Seconds (CSS) - In ESF mode, the number of seconds in an interval in which a controlled slip occurred.	0

Table D-12 3C Inband reports

Event	Default
Seconds in interval - elapsed time, in seconds	(counter)
FCS (Frame Check Sequence) - current count of the number of frames that have arrived with FCS errors.	(counter)
Overrun - overrun condition is detected by receiver. If receiver is unable to receive frames, because it does not have buffers to place the received frames. This condition occurs if the frames are received at a very high rate.	(counter)
Errored Seconds - a second with one or more frame errors	(counter)
Discarded frames - current count of thrown-away data blocks	(counter)
Received packets - current count of arrived data packets	(counter)
Received octets - current count of arrived data bits	(counter)
Received Usage - the octet arrival rate as the percentage of the link speed. RxUsage = (rxOctets•B)•100/dataRate•timeInterval)	(value)
Transmitted packets - current count of sent data blocks	(counter)
Transmitted octets - current count of sent data bits	(counter)
Transmitted Usage - the octet transmission rate as the percentage of the link speed. TxUsage = (txOctets•B)•100/dataRate•timeInterval)	(value)

Table D-13 Menu-3EA DLCI Outages

Indication	Description
DLCI	Identifies the DLCI.
Outage State	Outage State may be Included, Excluded, or None.
Included Outage	These columns present data collected on unscheduled service outages. The Count column provides the number of INcluded outages on the DLCI since the last reset. The Time column provides the number of unscheduled minutes the DLCI was down.
Excluded Outage	These columns present data collected on outages that are scheduled or unavoidable. These outages include down time scheduled for maintenance, and down time attributable to acts of nature such as flood. The Count column provides the number of Excluded outages on the DLCI since the last reset. The Time column provides the number of minutes the DLCI was down due to an Excluded outage.

Table D-14 Menu-3EB Frame Transfer Delays Report Definition

Indication	Description
DLCI	Identifies the DLCI.
Last Sample Time	The time of the most recent sample.
Threshold Violations	The number of times the delay threshold has been exceeded.
Total Samples	The number of samples that have been taken.
Average Delay	Average Delay is calculated by taking the sum of the total delay and dividing it by the number of samples collected.
Maximum Delay, Last n Samples	This column is subdivided into three columns. Here you will find the single longest delay during the last 15 samples, 30 samples, and 60 samples.

Table D-15 Menu-3EC Local Transmit Data Delivery Report Definitions

Indication	Description
DLCI	Identifies the DLCI.
Last Sample Time	The time of the most recent sample.
Threshold Violations	The number of times the DDR threshold has been exceeded.
Local Transmit Within CIR	The number of bytes transmitted within CIR.
Local Transmit Above CIR	The number of bytes transmitted above CIR.
Far End Within CIR	Number of bytes received at far end within CIR.
Receive Above CIR	Number of bytes received at far end in excess of CIR.

Table D-16 Menu-3EE Local Receive Data Delivery Report Definitions

Indication	Description
DLCI	Identifies the DLCI.
Last Sample Time	The time of the most recent sample.
Threshold Violations	The number of times the DDR threshold has been exceeded.
Local Receive Within CIR	The number of bytes received within CIR.
Local Receive Above CIR	The number of bytes transmitted above CIR.
Far End Transmit Within CIR	Number of bytes transmitted within CIR from the far end.
Far End Transmit Above CIR	Number of bytes transmitted in excess of CIR from the far end.

Table D-17 Menu-3EF Local Transmit Frame Relay Delivery Report

Indication	Description
DLCI	Identifies the DLCI.
Last Sample Time	The time of the most recent sample.
Threshold Violations	The number of times the DDR threshold has been exceeded.
Local Transmit Within CIR	The number of frames transmitted within CIR.
Local Transmit Above CIR	The number of frames transmitted above CIR.
Far End Within CIR	Number of frames received at far end within CIR.
Receive Above CIR	Number of frames received at far end in excess of CIR.

Table D-18 Menu-3EG Local Receive Frame Delivery Report

Indication	Description
DLCI	Identifies the DLCI.
Last Sample Time	The time of the most recent sample.
Threshold Violations	The number of times the DDR threshold has been exceeded.
Local Transmit Within CIR	The number of frames transmitted within CIR.
Local Transmit Above CIR	The number of frames transmitted above CIR.
Far End Within CIR	Number of frames received at far end within CIR.
Receive Above CIR	Number of frames received at far end in excess of CIR.

Table D-19 Menu-3FA Ethernet physical layer

Parameter	Description
FCS Errors	FCS errors
Single Collisions	Total number of single collisions
Defer Transmit	Total number of deferred transmissions
Late Collisions	Total number of late collisions
Carrier Sense Errors	Total number of carrier sense errors
Frames Too Long	Total number of frames received that are too long

Table D-20 Menu-3FB Ethernet interface statistics

Parameter	Description
Octets Received	Total number of octets received
Octets Transmitted	Total number of octets transmitted

Parameter	Description
Unicast Packets Received	Total number of unicast packets received
Unicast Packets Transmitted	Total number of unicast packets transmitted
Non Unicast Packets Received	Total number of non-unicast packets received
Non Unicast Packets Transmitted	Total number of non-unicast packets transmitted
Unknown Protocol ID	Protocol ID unknown
Protocol Packet Dump	Total number of Rx packets received with Ethernet errors
Unroutable Packets	Total number of unroutable packets received

Table D-21 Menu-3FC IP Statistics

Parameter	Description
Packets Received	Total number of packets received
Header Errors Received	Total number of packet header errors
Address Errors Received	Total number of packet address errors
Forwarded Datagrams	Total number of forwarded datagrams
Unknown Protocol Received	Total number of packet unknown protocols
Discards <Rx>	Total number of packet discards received
Discards <Tx>	Total number of packet discards transmitted
Packets Delivered	Total number of In-band packets received
Requests Transmitted	Total number of requests transmitted
Reassembly Required	Total number of packet fragments requiring reassembly
Reassembly Successful	Total number of successful packet reassemblies
Reassembly Failed	Total number of failed packet reassemblies
Fragmentation Successful	Total number of successfully fragmented IP packets
Fragmentation Failed	Total number of packet fragments failed
Fragments Created	Total number of packet fragments created

Table D-22 Menu-3FE ICMP receive statistics

Parameter	Description
Messages Received	Total number of messages
Errors Received	Total number of packet header errors
Destination Unreachable (Rx)	Total number of unreachable destination messages
Time Exceeded (Rx)	Total number of packets with time exceeded
Parameter Problems (Rx)	Total number of packets with parameter problems
Source Quench (Rx)	Total number of packets with source Quenches
Redirects (Rx)	Total number of packet redirects

Parameter	Description
Echos (Rx)	Total number of packet echo requests
Echo Replies (Rx)	Total number of packet echo replies
TimeStamps (Rx)	Total number of packet timestamp requests
TimeStamp Replies (Rx)	Total number of packet timestamp replies
Address Masks (Rx)	Total number of packet address masks requests
Address Mask Replies (Rx)	Total number of packet address masks replies

Table D-23 Menu-3FF ICMP Transmit statistics

Parameter	Description
Messages Transmitted	Total number of messages
Errors Transmitted	Total number of errors
Destination Unreachable <Tx>	Total number of packets with unreachable destinations
Time Exceeded <Tx>	Total number of packets with time exceeded
Parameter Problems <Tx>	Total number of packets with parameter problems
Source Quench <Tx>	Total number of packet source Quenches
Redirects <Tx>	Total number of packet redirects
Echos <Tx>	Total number of packet echo requests
Echo Replies <Tx>	Total number of packet echo replies
TimeStamps <Tx>	Total number of packet timestamp requests
TimeStamp Replies <Tx>	Total number of packet timestamp replies
Address Masks <Tx>	Total number of packet address masks requests
Address Mask Replies>	Total number of packet address masks replies

Table D-24 Menu-3FG ARP Statistics

Parameter	Description
Requests Received <All>	Total number of ARP requests received
Requests Received <For Me>	Total number of requests received from me
Replies Sent	Total number of ARP replies sent
Replies Received	Total number of ARP replies received
Requests Sent	Total number of ARP requests sent

Table D-25 Menu-3M Delay Monitoring

Indication	Description
Avg	Average delay in milliseconds
Max	Maximum delay

Indication	Description
Lost	number of packets lost
Bad	number of packets with checksum errors.
Set	number of packets transmitted

Table D-26 Menu-3Z Event Log

Parameter	Description	Default
Module	Unit, Network, System, All This field allows the display of any of the above status changes. When Unit is selected, the following status changes will be logged as events:	All
Event	Unit Power On Self Test Net Loopback (port) Payload Loopback (port, fraction) Loop Up Remote (port, fraction) Loop Down Remote (port, fraction) Send User 1 Pattern (port, fraction) Send User 2 Pattern (port, fraction) Send 1:1 Pattern (port, fraction) Send 1:2 Pattern (port, fraction) Send 1:4 Pattern (port, fraction) Send 1:7 Pattern (port, fraction) Send 3:24 Pattern (port, fraction) Send QRW Pattern (port, fraction) Send All 1's Pattern (port, fraction) Send All 0's Pattern (port, fraction) No Clock Lamp Test Send Keep Alive Controlled Slip Inject a Pattern Error Clear Pattern Error Counter Clear Event Log Clr Current Carrier Registers Clear Carrier Archives Clear Current User Registers Clear User Archives Clear User CRC Errors Clear User BPV Errors Clear User OOF Errors Clear All User Error Counters Clear 24 Hour User Registers Back to Factory Config	

Parameter	Description	Default
Event (cont.)	Loss of Signal Loss of Frame Set Code Received Reset Code Received UA1 Received CV Threshold Exceeded FE Threshold Exceeded CRC Threshold Exceeded External ALarm Asserted Power Outage UAS Outage Flash N.V. Log Error Clear User 4 Day Archive Clear User 14 Day Totals	
Module	When **All** is selected, all of the preceding status changes will be logged as events.	
	When **Network** is selected, the following status changes will be logged as events: Network Loss of Signal Loss of Frame Set Code Received Reset Code Received BPV Threshold Exceeded CRC Threshold Exceeded OOF Threshold Exceeded	
	When **AUX** is selected, the following status changes will be logged as events: Loss of Signal Loss of Frame	
Module	When **System** is selected, the following status changes will be logged as events. External Alarm Power Supply Failure	
Event	This field allows a particular type of event to be displayed Enter an event index or use the Up/Down keys to scroll through the event options. While selecting the event, the event description text changes with the index. The event description text is displayed under the Description column in the Event Log menu. If the Event field is left blank, the Event filter parameter is disabled.	0, All
Seq. No.	This value uniquely identifies an event in a certain unit. This field is read only.	
Status	Identifies the condition of the event described in the description field. This field is read-only.	
Module	Identifies the module type. This field is read-only.	
Description	Identifies the status change/event. This field is read-only.	

Parameter	Description	Default
Time/Date	Identifies the time the status change/event was logged.	

Table D-27 Menu-4A Unit Configuration

Parameter	Description
UNIT	**Protect Mode** - Enabled or Disabled; Enabled - Protect mode prevents you from running tests from the front panel.
	Yellow Alarm - Enabled or Disabled; Enabled - The unit detects and generates a Yellow Alarm. Disabled - The unit does not detect or generate a Yellow Alarm.
NETWORK	**Main/Alt Sync -** INT, NET1, NET2 Selects the E1 network transmitter's clock source. First specify the Main clock source value, then the Alternate. (Each clock source has the same options.) Type **y** to confirm each action. **NET**: Select this option if the network is the clock source. If it is not, set to Int at one E1 end, and NET at the other end.

Table D-28 Menu-4B Net Configuration and status

Parameter	Description
NET 1/2	**Framing** Selects the Network T1/E1 framing format. **E1:** CRC4 enabled, CRC4 disabled, and unstructured (
	Line Impedence View setting of E1 line impedence (75 ohm or 120 ohm)

Table D-29 Menu-4T GMT Time synchronization

Parameter	Description
Time/Date	**Automatic Sync** Set automatic synchronization to Enabled or Disabled. **Default:** Disabled
How Often	Set the frequency of how often to synchronize the time with the time server (Days, hours, minutes, seconds)
Next sync	Displays synchronization count down and next scheduled synchronization
Time Src	Configure primary and secondary time server IP addresses and port of which time servers are connected
Attempts	Displays count of access attempts to time server

Table D-30 Menu-4V Timezone configuration

Parameter	Description
Ahead GMT	Set this to Yes if unit is deployed to the east of GMT. Set NO if the unit is deployed in to the west of GMT.
Hrs. Offset From GMT	Offset hours from GMT from 0 to 23
Mins. Offset From GMT	Offer minutes from GMT from 0 to 59l
DST	Enable or disable Daylight Savings Time. Set to Enable If user's timezone supports Daylight Savings Time.
Hrs. of Difference during DST	Number of hours saved during Daylight Savings Time
Mins. of difference during DST	Number of minutes saved during Daylight Savings Time
DST Start week	Week of the month in which Daylight Savings Time starts
DST Start month	Month when Daylight Savings Time starts.

Table D-31 Menu-6A PPP/MLPPP Configuration Parameters

Parameter	Description
Keepalive Timer	Controls the messages of the keepalive (echo request) messages after the link(s) is(are) negotiated
Keepalive Timeout	Controls how long an end point should wait for "ech response" after ending "echo request"
Retry Counter	How many unsuccessful "echo requests" should be attempted before a link is declared down

Table D-32 Menu-6A Multilink Frame Relay Configuration Parameters

Parameter	Description	Default
MFR	**Link Integrity Timer** - controls rate of MFR protocol messages	10
	Link Acknowledge - controls rate of MFR protocol acknowledgement messages	4
	Retry Counter - number of retransmission attempts for MFR protocol	2
	Discarded Frames - (status) number of invalid MFR frames discarded	(counter)
Local	**Local Bundle Identifier -** (status) local identifier for logical T1 bundle	(ID no.)
	Remote Bundle Identifier - (status) remote identifier for logical T1 bundle	(ID no.)

Table D-33 Menu-6B PPP/MLPPP Port Status

Parameter	Description
Port 1/2	**Include In Service** - Yes, No
	Status - Normal, Idle, Down, and Loopback Detected

Parameter	Description
	Protocol Error - Number of PPP/MLPPP protocol errors detected in this port.

Table D-34 Menu-6B Multilink Frame Relay Port Configuration and Status

Parameter	Description	Default
Port 1/2	**Include In Bundle** - Yes, No	Yes
	Status - Normal, Idle, Down, Remote Not Configured, Inconsistent Bundle, Unknown Vendor, Loopback Detected, Test Active, Remote Link Up, and Awaiting Remote Link	(status)
	Protocol Errors - number of MFR protocol errors detected on the port	(counter)
Local	**Local Bundle Identifier -** (status) local identifier for logical T1 bundle	(ID no.)
	Remote Bundle Identifier - (status) remote identifier for logical T1 bundle	(ID no.)

Table D-35 Menu-7 Feature Keys

Parameter	Default
RMON – PPP and Frame Relay RMON1 statistics	Capable
Service Level Agreement (Frame Relay SLA FRF.13)	Capable
RMON 2 - Protocols and application monitoring	Capable
Access Router 2 Ports –	Capable
Access Router single port	Not capable
Dynamic Routing --	Capable

Table D-36 Alarm Configuration

Primary Parameters	Parameter—Options; Definition	Default
NET Alarms	**Block All Alarms**—Yes, No Yes—Blocks the reporting of all alarms. No—Enables the unit to report alarms.	No
	Carrier Loss Alarm—Enabled, Disabled Enabled—The unit generates an alarm when a network carrier Loss of Signal is detected on the network. Disabled—Disables the alarm.	Enabled
	Sync Loss Alarm—Enabled, Disabled Enabled—The unit generates an alarm when loss-of-frame is detected on the network. Disabled—Disables the alarm.	Enabled

Primary Parameters	Parameter—Options; Definition	Default
NET Alarms	**AIS Received Alarm**—Enabled, Disabled Enabled—The unit generates an alarm when a Network AIS (Alarm Indication Signal) is detected. Disabled—Disables the alarm.	Enabled
	RAI Received Alarm—Enabled, Disabled Enabled—The unit generates an alarm when a Network RAI Alarm is detected. Disabled—Disables the alarm.	Enabled

Table D-37 Menu-8C Miscellaneous Management Configuration

Parameter—Options; Definitions
Connection—In-band, Modem, Direct Select the type of connection you are using. In-band—Enables an in-band connection to the unit. Modem—Enables a modem connection to the unit. Direct—Enables a direct terminal connection to unit.
Timeout When Logged On—1 Min, 10 Min, 30 Min, Unlimited Applies only when you are logged on. This is the time span after which, if it does not detect activity, the system warns that you will be logged off in 30 seconds.
Timeout When Not Logged On—1 Min, 10 Min, 30 Min, Unlimited Applies only when a terminal is connected through a modem and you are not logged on.This is the time span after which the modem disconnects the phone line if no activity is detected.
Phone Number 1 Enter a Hayes-compatible modem dial string (20 char. maximum); for example, “atdt555-1212”. The modem dials out using the first telephone number, then automatically tries the second telephone number if the first does not respond.
Phone Number 2 Enter a Hayes-compatible modem dial string (20 char. maximum); for example, “atdt555-1212”.
Normal User Password—(text string) Enter the login password for the Normal User (20 char. maximum).
Super User Password—(text string) Enter the login password for the Super User (20 char. maximum).
DLC IBC Link Loss Alarm—Enabled or Disabled The IBC link specific to Dual Trunk E1 Router. When the connection is disrupted, an alarm is sent.
Dial Out Time Interval—Dial out time interval is the minimum amount of time the Dual Trunk E1 Router waits between dial outs to the host computer.
In-band Link Loss Alarm—Enabled or Disabled Enabled—When loss of HDLC frames or idle characters occurs, an alarm is generated. Disabled—The alarm is disabled

Parameter—Options; Definitions
In-band CRC Error Threshold—Enable or Disabled Enabled—The valid range for this is 4 x 10^{-7} to 9 x 10^{-1}. Disabled—No alarm is generated if threshold rate of errors is high.

Table D-38 Menu-8E Modem Initialization Strings

Parameter	Default
String 1 – Modem initialization string can be up to 20 characters.	N/A
String 2 – Modem initialization string can be up to 60 characters.	N/A

Table D-39 Menu-8F Comm Port configuration

Parameter	Default
COMM PORT – Baud Rate Parity Word Length Stop Bits	38400 None 8 2
DCD – Enabled or Disabled Enabled – The Multilink Select uses the modem's Data Carrier Detect (DCD) signal to provide more robust modem operation. Disabled – Use Disabled if your null modem does not pass the Data Carrier Detect signal.	Disabled
XON/XOFF – Disabled, XOFF until ANY, XOFF until XON XOFF until ANY – Ctrl-S stops data flow from unit, any key resumes data flow. XOFF until XON – Ctrl stops data flow from unit, Ctrl-Q resumes flow. Disabled – XON/XOFF feature disabled.	Disabled

Table D-40 Menu-9A Physical layer diagnostics

Field	Definition — Options	Default
Choosing a test by number	You may type in a number to select a test, instead of using the arrow keys. For instance, if you type in "3," you will select the Net Lpbk test.	
Current Test	Displays the test currently running. If no test is selected, the field reads `Idle.`	Idle
Pattern Test	If no pattern test is running, the test reads `idle`. When a pattern test is started, it will read `Searching`. When the current pattern test is locked, it displays `locked seconds. Locked seconds` is a 16-bit counter saturating at 65536. The counter resets to 0 when the current pattern is lost. The counter label will change to `Relocked Seconds` if the current pattern is lost and found again. Options: Idle, Searching, Locked, and Relocked	

Field	Definition — Options	Default
Pattern Error Counter	The number of pattern errors occurring during the current test. This will only display when Pattern Test reads `Locked Seconds` or `Relocked Seconds.`	0
CRC (or CRC4) Errors	The number of CRC (or CRC4) errors occurring during the current test.	0
Code Violations	The number of Code Violations occurring during the current test.	0
Out of Frame Event	Indicates 2 bits out of 4 bits framing errors for both ESF and D4 modes	0
Frame Error Event	Indicates 2 bits out of 4 bits framing errors	0
Last Self Test Result	The result of the last test performed. Read only. Options: Self Test Passed Error nn (0 to 5)	0 (if no self-test has been performed)
Next Test (port, fraction)	The next test to run is set in this field. Options: 1. Self Test† 3. Loop NET 4. Loop Payload* 5. Loop Up Remote * 6. Loop Down Remote* 7. QRW Pattern* 8. 1:7 Pattern* 9. 3:24 Pattern* 10. 1:1 Pattern* 11. All 1s Pattern* 12. All 0s Pattern* 13. 1:2 Pattern* 14. 1:4 Pattern* 15. User 1 Pattern* 16. User 2 Pattern* 17. Smart Jack Set‡ 18. Smart Jack Reset‡ 19. Lamp Test† *All of these tests offer the option of selecting which fraction of the T1/E1 signal the test applies to (NET1, NET2). FULL applies to the entire T1/E1 signal (including IDLE timeslots).	Self Test
Next Test Length	The length of the next test is set in this field. 15 min., 1 min., 60 min., Unlimited With the Self Test, Loop Up Remote and Loop Down Remote, this parameter does not apply.	Unlimited
Full Bandwidth Loop Code	The Loop code to use in the next test is set in this field. Options: Standard, Alternate, Disabled	Standard
Fractional Loop Code	The Loop code to use in the next test is set in this field. Options: Standard, Alternate, Disabled, and ITU-T V.54	Standard

Field	Definition — Options	Default
USER 1 Pattern and USER 2 Pattern	Enter any sequence of 1s and 0s, between 1 and 24 characters in length. With D4 framing, make sure your pattern meets density requirements. The parameters and options in the upper test status section of Menu-9 Diagnostics are given next.	1 — 001100110011001 100110012— 000100010001000 10001000

Table D-41 Menu-9B Link Layer diagnostics options

Type	Parameter — Definition	Default
Current	**Test** — The test that is currently running. Display only.	Idle
	Link — The IP address, DLCI and Port on which the test is currently running. Display only.	Empty
Status	**Sent Packet** — The number of packets sent in the current test. Display only.	0
	Received Packets — The number of packets received in the current test. Display only.	0
	Errored Packets — The number of packets containing errors sent in the current test. Display only.	0
Status	**Missing Packets** — The number of packets that were lost in the current test. Display only.	0
	Average Round Trip — The average length of the round trip from local to remote in the current test. Display only.	0

Type	Parameter — Definition	Default
Next	**Test** — Selects the type of test to run next. Options: Ping 511 Ping 1023 Ping 2047 Ping 1:1 Ping All 1s Ping All 0s	Ping 511 pattern
	IP Address — nnn.nnn.nnn.nnn The IP address on which the test is to be run.	0.0.0.0
	DLCI, Port — The DLCI and Port out which the test is to be run. The DLCI specified must be between 0 and 1024. The port can be NET, DTE, ENET, and COMM.	16,NET
	Test Length — The number of minutes the test is to last. Selecting a length of zero will choose unlimited duration.	0
	Test Interval — The number of seconds between test packets.	0
	Packet Size — The size of the packet sent in the test.	100

Table D-42 Menu-9C Delay Monitoring configuration

Parameter-Definition	Default
State Enables or disables Delay Monitoring on the link.	Not Running (disabled)
Pattern The test pattern in the ping packet.	Ping 511 Pattern
DLCI, Port The DLCI and Port on which the test is to be run. Port options: NET, DTE, Ethernet, and COMM.	16, NET
Test Interval Interval size in seconds between transmission of test packets	60
Packet Size The size of the test packets.	100

Table D-43 Menu-$A Unit Configuration

Primary Parameter	Parameter–Options; Definition	Default
UNIT	**Packet Processing Mode** – can be set to Fast Forwarding, Fast Forward Broadcast, or Routing	Routing

Primary Parameter	Parameter–Options; Definition	Default
	Default Gateway IP Address - default IP address	0.0.0.0
	Default Gateway - enable or disable Gateway	Disabled
	Firewall – enable or disable firewall	Disabled
	Load Balancing – enable or disable Load Balancing	Disabled

Table D-44 Menu-$B Display routing table

Indication	Description
Destination IP/Len	Destination IP or network address/length
Next Hop IP	Next IP/network address along the route
Interface	Interface (Self, ENET, MLPPP, PPP1, PPP2) on which packet will be sent
Flags	Indicates type of route (Connect, Static)
Metric	Distance to next Gateway enroute to destination IP

Table D-45 Menu-$C Static routing table parameters

Indication	Description
Status	Shows routes active or inactive
Destination IP/Len	Destination IP or network address
Next Hop IP	Next IP/network address along route path
Interface	Interface (Self, ENET, MLPPP, PPP1, PPP2) on which packet will be sent
Metric	Distance to next gateway enroute to destination IP
Action	Add or delete route

Table D-46 Menu-$F Display ARP Table

Address	Definition
IP Address	Address for client or server station (0.0.0.0)
MAC Address	Address for LAN network card

Table D-47 Menu-$H Firewall table

Indication	Definition
Ord	Order number in which packet is processed
Action	Permit or Deny - processing of packet is either permitted or denied
Src Address/Len	Packet source address/length
Dest Address/Len	Packet destination address/length
SrcIntf	Packet source interface (ENET, MLPPP, PPP1, PPP2)

Indication	Definition
Status	Status is either Active or Inactive. Press the “k” key (see bottom of screen) to save the Status to the Firewall Table.

Table D-48 Menu-$K DHCP Relay configuration

Parameter	Definition
DHCP Relay	Enable or disable DHCP relay agent
DHCP Server	DHCP Server IP address

Dual Trunk E1 Router

Router Command Line Interface Reference

ACCESS TO ROUTER COMMAND LINE

The Dual Trunk router command line interface (CLI) is accessible manually via TUI and programmatically for configuring the router automatically.

For manual configuration and troubleshooting, access the CLI via the TUI Menu-$E directly through the COMM port, or Telnet via the Ethernet or the WAN ports. You enter the commands one line at a time using the command syntax outlined in this appendix.

Configuring the router automatically

You can manage your router configurations using configuration files. Retrieve the complete router configuration onto an ASCII text file and store it on a server for backup. Make changes to the router configuration file off-line then download it either manually or automatically. The following table lists the procedures for retrieving and saving, and downloading router configuration files..

Table E-1 Router automatic configuration procedures

Procedure	Steps
Retrieving and saving the router configuration to a file	To retrieve the router configuration file, you will need to access the router TUI, display the router configuration on the Terminal or Telnet session, then cut and paste to an ASCII text file. 1.Select Menu-8X from the TUI 2.Enter **B** to select the command **Display Configuration** 3.Enter Y to the prompt “Start Configuration Display (Y/N) ?” The router will display the complete router configuration using CLI commands 4.From your Terminal Window or Telnet session, cut and paste the displayed router configuration to an ASCII text file, then save the file.
Downloading router configuration manually	You can download a router configuration file containing either a complete router configuration or partial changes to the router configuration. 1.Select Menu-8X from the Terminal User Interface 2.Select the download method TFTP or Xmodem 3.Answer Y to the prompt “Do you really want to change to router configuration (Y/N) ? 4.From your Workstation, select the router configuration file and start the TFTP or Xmodem download

Table E-1 Router automatic configuration procedures

Procedure	Steps
Downloading router configuration automatically	You can initiate the configuration file download programmatically using SNMP commands, and use TFTP or Xmodem method to download the file. Menu-8X Router auto configuration commands and options are accessible via SNMP variables in the eclipse MIB. The following shell script sample shows a TFTP download of a router configuration file called "site_a.txt": #!/bin/ksh NODE="172.25.150.1" AUTO_FILE="site_a.txt" snmpset $NODE .1.3.6.1.4.1.300.200.2.50.1.0 integer 1 tftp $NODE <<EOT bin put $AUTO_FILE quit EOT snmpget $NODE .1.3.6.1.4.1.300.200.2.50.10

ROUTER COMMAND LINE HELP

The CLI contains a text-based help facility. Access this help by typing in the full or partial command string then typing "?". The CLI displays the command keywords or parameters for the command plus a short description.

For example, at the CLI command prompt, type show? (the CLI does not display the question mark). The CLI displays this keyword list with short descriptions for each keyword:

```
debugging  Zebra configuration
history    Display the session command history
interface  Interface status and configuration
ip         IP information
```

```
memory      Memory statistics
```

Table E-2 Router CLI Help

Topic	Description
Syntax Help	Use command **?** to list commands or use **List** command to see available commands for each each mode. At the CLI command prompt type kernel: [Unit/Kernel/Rip/Ospf/Bpg]#kernel [Kernel(enable)]# sh ? Press TAB. The CLI shows: [Kernel(enable)]# show Type `show i`. Press TAB. The CLI shows: [Kernel(enable)]# show i interface ip [Kernel(enable)]# show i The CLI waits for your choice of the `interface` or `ip` parameters. Type `n` and press TAB. The CLI shows: [Kernel(config)]# show in [Kernel(config)]# show interface Type? and the CLI shows the list of parameters for the `show interface` command. This command has one positional parameter, an interface name. [IFNAME] Interface name [Kernel(enable)]> show interface The router waits for you to supply a value for the IFNAME parameter.
Coomand abbreviations	The CLI accepts abbreviations for commands. For example, sh in is the abbreviation for the show interface command.
Command line errors	If at any time the router does not recognize the command or parameter (check the position of a parameter) it displays this message: % Unknown command. If a command is incomplete it displays this message: % Command incomplete. Some commands are too long for the display line and can wrap in mid-parameter or mid-keyword if necessary: area 215.216.217.218 virtual-link 215.216.217.218 authentication-key 57393
Command Negation	In this example from the OSPF `area virtual-link` command, `no` is optional. This means that the entire syntax can be negated. Depending on the command or the parameters, command negation can mean the disabling of one entire feature for the router or the disabling of that feature for a specific ID or address. (no) area AREAADDRESSID virtual-link ROUTERID (AUTHENTICATE|MSGD|INTERVAL) In this example negation is for the base command; the negated command does not take any parameters. default-metric <1-16777214> no default-metric

Table E-2 Router CLI Help

Topic	Description
Parameter expansion	For the area `virtual-link` command, the `AREAADDRESSID` parameter is replaced by either an IP address or a number in the given range: AREAADDRESSID=A.B.C.D|<0-4294967295> The minimum command then is: area 1.1.1.1 virtual-link 2.2.2.2 The parameters in the string `(AUTHENTICATE|MSGD|INTERVAL)` are optional. Each one of which is replaced by more keywords and values.

CLI Command Modes

The commands available are divided in three categores (Unit, Kernel, and Routing) and arranged in a hierarchy. Each of the three modes has its own set of commands and its own sub modes of hierarchy.

The commands available for each routing protocol (RIP and OSPF) are separated into several modes and arranged in a hierarchy. Enable is the default mode and is the lowest level. Each mode has its own special commands; in some modes, commands from a lower level are available..

Table E-3 CLI command modes

Mode	Description
Enable	This mode is the base mode from where users can perform basic commands like show, exit, quit, help, list, enable. This mode also includes some debugging command, the save commands (for saving and viewing the configuration), show protocol specific information, and so on. Enable is the default mode.
Configure	Sometimes referred to as Configure Terminal, this mode serves as a gateway into the Interface and Router.
Interface	This mode makes protocol-specific configuration commands accessible.
router	Sometimes referred to as configure-router mode, this mode available for the RIP and OSPF protocols, makes available router and routing commands.
Line	Used for access-class commands. It is available for the OSPF and RIP protocols.
Route-map	Mode used to set route metric, route-length and cost data. It is available for the OSPF and RIP protocols.

When you enter the CLI, the following prompt is displayed:

Access Router CLI, type

Unit to enter Unit mode

Kernel to enter kernel mode

Rip to enter RIP mode

Ospf to enter OSPF mode

Quit to exit

[Unit/Kernel/Rip/Bgp/Ospf]:

When you enter Unit the prompt will change to: Unit(enable)

```
[Unit/Kernel/Rip/Bgp/Ospf]: unit
Unit(enable)#
```

When you enter Kernel the prompt will change to: KERNEL(enable)

```
[Unit/Kernel/Rip/Bgp/Ospf]: Kernel
Kernel(enable)#
```

Enter quit to go back to the top level

```
Kernel(enable)#quit
[Unit/Kernel/Rip/Bgp/Ospf]:
```

Enter Rip to enter rip command mode

```
[Unit/Kernel/Rip/Bgp/Ospf]: rip
rip(enable)#
```

Enter bgp to enter BGP command mode

```
[Unit/Kernel/Rip/Bgp/Ospf]: bgp
bgp(enable)#
```

NOTE: Standard LRU4240 includes RIP1, RIP2, and OSPF dynamic routing. BGP-4 protocol is available as an optional dynamic routing protocol.

UNIT COMMAND REFERENCE

Unit mode lets you access the device unit E1, and Ethernet port physical interface settings, Frame Relay protocol, static routes, firewall, NAT, bridging, multilink, time synchronization, alarms, COMM port, and management interfaces.

configure terminal

Use the **configure terminal** command to change to configure terminal mode.
Command Syntax: **c**onfigure terminal
Command Mode: Enable
Usage
There are no arguments or keywords for this command. The prompt will change to
Unit(config)#
Example
Unit(enable)#configure terminal
Unit(config)#

quit

Use the **quit** command to change exit from the current mode and return to the higher level mode.
Command Syntax: quit
Example
Unit(config)#**quit**
Unit(enable)#

show running-config

Use the **show running-config** command to show running config.
Command Syntax
show running-config
Command Mode: unit
There are no arguments or keywords for this command.
Examples

```
 Unit(enable)#show running-config
show running-config
Use the show running-config command to show running config.
Command Syntax
show running-config
Command Mode: rip
There are no arguments or keywords for this command.
Examples
 Rip(enable)#show running-config
 43: Current configuration:
 44: !
 45: !
 46: !traffic configuration
 47: traffic type ppp
 48: multilink no
 49: traffic monitoring disabled
 50: ip route mode routing
 51: !
 52: !unit configuration
 53: unit protect-mode disabled
 54: unit yellow-alarm disabled
 55: unit clock primary net1
 56: unit clock secondary int
 57: unit remote-comm none
 58: unit ansi-fdl enabled
 59: unit monitor-jack net1
 60: !
 61: !net configuration
 62: t1 framing net1 esf
 63: t1 lbo net1 0db
....
```

show unit id

Use the **show unit id** command to show the 6 characters local unit identifier.
Command Syntax
show unit id
Command Mode: unit

There are no arguments or keywords for this command.

Examples

```
Unit(enable)#show unit id
 19: unit id SUNN1
```

e1 framing

Use the **e1 framing** command to configure the network E1 framing format.

Command Syntax: e1 framing [net1 | net2 | aux] [unstructured | crc-enabled | crc-disabled]

Command Mode: Config

Example

unit(config)#e1 framing net1 unstructured
unit(config)#

e1 line-impedance

Use the **e1 line-impedance** command to configure the network port line impedance to 75 or 120 ohms. This command is reserved for BlackBox personnel only, as it requires changing jumper settings on the hardware unit.

Command Syntax: e1 line-impedance [net1 | net2 | aux] [120-ohm | 75-ohm]

[net1 | net2 | aux] select the network port
120-ohm set line impedance to 120 ohm
75-ohm set line impedance to 75 ohm

Command Mode: Config

Example

unit(config)#e1 line-impedance net1 120-ohm

e1 timeslot

Use the **e1 timeslot** command to allocate an E1 timeslot and assign it to data, voice or idle.

Command Syntax: e1 timeslot <1-31> [aux | f1 | idle]

<1-31> select an E1 timeslot number
aux Assign selected timeslot to auxiliary dro-and-insert port
f1 Assign selected timeslot to Ethernet data port
idle Selected timeslot will not be used

Command Mode: Config

Example

Assign timeslot 10 to transport data from Ethernet data port.
unit(config)#e1 timeslot 10 f1

interface IFNAME icmp-redirect

Use the **interface IFNAME icmp-redirect** command to enable or disable ICMP redirect messages on the named interface

Command Syntax: interface [enet | net1 | net2 | bundle0] icmp-redirect [disabled | enabled]

disabled Do not send ICMP redirect messages on this interface
enabled Send ICMP redirect messages on this interface

Usage

ICMP redirect should be configured on the Ethernet interface only.

Command Mode: Config

interface IFNAME ip-addr

Use the **interface IFNAME ip-addr** command to set the interface IP address and subnet mask

Command Syntax: interface [enet | net1 | net2 | bundle0 | comm] ip-addr <A.B.C.D>/<Len>

enet Ethernet port
net1 Network port 1
net2 Network port 2
comm COMM port
bundle0 multilink interface, in multilink mode

<A.B.C.D> IP address in standard form
<Len> The subnet mask 1 to 32, the part of the IP address shared by all devices on the network.
Command Mode: Config

interface enet

Use the **interface enet** command to set ethernet port parameters including mask length, half or full duplex mode, and promiscuous mode
Command Syntax:
interface enet bcast-mask <1-32>
Set the mask length for Net directed IP broadcast in Fast Forwading mode.
Usage: Use this command in IP Fast Forwarding mode only.

interface enet data-mode [full-duplex | half-duplex]
Set physical data mode to half or full-duplex.

interface enet fwd-multicast [disabled | enabled]
Enable or disable forwarding of multicast packets in IP Fast Forwarding mode.
Usage: This command is applicable in Fast Forwarding mode only.

interface enet promiscuous [disabled | enabled]
To enable or disable promiscuous mode in Bridging mode.
Usage: Use this command in Bridging mode only.

interface enet proxy-arp [disabled | enabled]
To enable or disable proxy-arp in Fast-forwarding mode.
Usage: Use this command in Fast Forwarding mode only.

interface frame-relay dlci

Use the **interface frame-relay dlci clear** command to enter the DLCI number for a virtual cirtuit idendifier and the network port on which this DLCI is connected.
Command Syntax: interface frame-relay dlci <16-1023> [net 1 | net2 | bundle0]
<16-1023> dlci range
net1, net2, or bundle 0 Network interface on which the DCLI is connected
Command Mode: Config
Example
Unit(config)#interface frame-relay dlci 20 net1

interface frame-relay lmi

Use the **interface frame-relay lmi** command to enable or disable LMI and configure LMI parameters.
Command Syntax: interface frame-relay lmi [disabled | enabled | enquiry-rx-timer | enquiry-tx-timer | full-status-count | max-lmi-errir | type | unit-location]

disabled Disable LMI Conditioning
enabled Enable LMI Conditioning
enquiry-rx-timer <5-30> Set the expected interval in 5 seconds increments between expected receive enquiry status message
enquiry-tx-timer <5-30> Set the interval in 5 seconds increments between the sending of a STATUS ENQUIRY and the receipt of a response.
full-status-count <5-30> Set the interval in 5 seconds increments between the sending of a STATUS ENQUIRY and the receipt of a response.
max-lmi-error <5-30> Set the interval in 5 seconds increments between the sending of a STATUS ENQUIRY and the receipt of a response.
unit-location [CPE | CO]

Command Mode: Config

Example
Unit(config)#interface frame-relay dlci 20 net1

interface frame-relay map

Use the **interface frame-relay map** to map IP subnets to DLCIs.
Command Syntax: interface frame-relay map A.B.C.D/M <16-1023> {net1 | net2 | bundle0]
A.B.C.D/M IP network address and subnet mask length
<16-1023> DLCI number to map to
net1, net2 or bundle0 Network interface to map to
Command Mode: Config
Example
Unit(config)#interface frame-relay map 10.10.10.120/5 200 net1

interface frame-relay map clear

Use the **interface frame-relay map clear** to clear the IP subnets to DLCIs mapping table.
Command Syntax: interface frame-relay map clear
Command Mode: Config
Example
Unit(config)#interface frame-relay map clear

ip bridge static-route

Use the **ip bridge static-route** to configure the static MAC bridge routes table. Each bridge static route identifies a physical WAN or LAN port on which to bridge the MAC address.
Command Syntax:
ip bridge static-route X:X:X:X:X [enet | net1 | net2 | bundle0
Use this command in PPP mode:
X:X:X:X:X Host MAC address to bridge
IFNAME the port on which to bridge the MAC address
]
ip bridge static-route X:X:X:X:X [enet | net1 | net2 | bundle0] dlci <16-1023>
Use this command in Frame Relay mode
X:X:X:X:X Host MAC address to bridge
IFNAME the port on which to bridge the host MAC address
dlci <16-1023> Frame Relay DLCI on which to bridge the host MAC address
ip bridge static-route clear
Clear the static MAC brige route table.

ip dhcp-relay

Use the **ip dhcp-relay** to configure the DHCP relay agent.
Command Syntax:
ip dhcp-relay [enabled | disabled]: Enables or disables DHCP relay agent
ip dhcp-relay server A.B.C.D: Set the DCHP server IP address
Command Mode: Config
Example

ip firewall

Use the **ip firewall** to configure the access list filtering packets by denying or permitting access from source hosts to destination hosts.
Command Syntax:
ip firewall [0-511] [deny | permit] A.B.C.D/M A.B.C.D/M [enet | net1 | net2 | bundle0] [active | inactive]
Enter up to 512 rules denying or permitting access.
ip firewall clear: Clear the firewall

Command Mode: Config
Example

ip nat

Use the **ip nat** to enable or disable NAT for each physical interface.
Command Syntax:
ip nat [enabled | disabled]
Global parameter enabling or disabling NATfeature.

ip nat IFNAME [nat | napt | two-way-nat] [enabled | disabled]
To specify and enable the type of nat per interface port.
Command Mode: Config
Examples
Enable nat on NET1 port and disable NAT on Ethernet port and NET2.
Unit(config)#ip nat net1 enabled
Unit(config)#ip nat net2 disabled
Unit(config)#ip nat enet disabled
Unit(config)#ip nat enabled

ip nat global

Use the **ip nat global** to configure the **public IP addresses** (Global) used by NAT for the **private ip addresses** (local-addr).
Command Syntax:
ip nat global A.B.C.D/M IFNAME
A.B.C.D/M: Global registered IP address with subnet mask
IFNAME the interface port [net1 | net2 | bundle0 | enet0] on which the global IP address is used
ip nat global clear: Clear the NAT global Map table
Command Mode: Config
Example

ip nat local-addr

Use the **ip nat local-addr** to configure the networks that require NAT translation. Refer to Menu-$C Local address table for more information.
Command Syntax:
ip nat local-addr A.B.C.D/M IFNAME
A.B.C.D/M: Local IP Network and subnet to translate
IFNAME the interface port [net1 | net2 | bundle0 | enet0] to which the the local IP network is attached.
ip nat local-addr clear: Clear the local address table
Command Mode: Config
Example

ip nat static

Use the **ip nat static** to configure static NAT one-to-one mapping of global IP address to local IP addresses.Static NAT corresponds to menu-$JB NAT Static table.
Command Syntax:
ip nat static A.B.C.D A.B.C.D IFNAME
A.B.C.D Local IP address to translate
A.B.C.D Translated IP address
IFNAME the [net1 | net2 | bundle0 | enet0] interface port
ip nat static clear: Clear Static NAT table
Command Mode: Config

ip route

Use the **ip route** command to set static routes that map destination IP addresses to next hop IP address or interface. Static routes can be edited, changed, viewed from menu$-JC.

Command Syntax:

ip route A.B.C.D/M IFNAME metric <0-255>

Static route mapping destination IP address to interface port

A.B.C.D/M Static route destination IP address field

IFNAME the [net1 | net2 | bundle0 | enet0] interface port

metric <0-255> Static route metric field in seconds

ip route A.B.C.D/M A.B.C.D metric [0-255]

Static route mapping destination IP address to next hop IP address

A.B.C.D/M Static route destination IP address field

A.B.C.D Next hop IP address

metric <0-255> Static route metric field in seconds

Command Mode: Config

ip route bridge-route-aging-time

Use the **ip route bridge-route-aging-time** command to set the bridge route aging time. This command is functional in bridging packet processing mode only.

Command Syntax:

ip bridge-route-aging-time <10-1000000>

ip route default-gateway

Use the **ip default-gateway** to specify the default router or next hop where IP datagrams will be forwarded if no routes are found. In Fast Forwarding mode, packets will be forwarded to the default Gateway on the Ethernet port if no host on the LAN responds. This command is applicable in bridging, fast forwarding, and routing mode. In routing mode you can also specify a default gateway by entering a static route with 0.0.0.0/0 as <nexthop>.

Command Syntax:

ip default-gateway [enabled | disabled]

ip default-gateway A.B.C.D: Set default gateway IP address

A.B.C.D Gateway IP address

Command Mode: Config

Example

ip route load-balancing

Use the **ip route load-balancing** to load balance traffic between two equal routes on two independent T1/E1 links.

Command Syntax:

ip route load-balancing [enabled | disabled]

Enable or disable load balancing. You will need to set two routes with equal cost to the same destination network on different interface (NET1, NET2).

Command Mode: Config

Example

ip route mode

Use the **ip route mode** to set packet processing mode to routing, bridging, or Fast Forwarding.

Command Syntax:

ip route mode [routing | bridging | fast-forward]

routing: In this mode packets will be routed to next hop address based on static and dynamic route tables.

bridging: Configures the unit for Bridging or VLAN bridging. This mode is commonly called MAC Bridging as the unit forwards Ethernet frames.

fast-forward: In this mode the unit forwards IP packets, not the Ethernet frames, over the WAN link.

Command Mode: Config

Example

ip route vlan-id

Use the **ip route vlan-id** to set the unit management VLAN ID. With the default VLAN ID disabled, set to 9999, the unit will check every VLAN frame for management traffic by matching the destination IP address with the unit IP address, which is the Ethernet port IP address. By setting a unit VLAN ID, the unit will first match VLAN ID in VLAN frames, then match the destination IP address with the unit IP address. This limits management traffic to a specific VLAN and reduces the processor load.

Command Syntax:

ip route vlan-id <0-4093>

Set the VLAN ID for management traffic.

Command Mode: Config

Example

ip route vlan-priority

Use the **ip route vlan-priority** to set the unit VLAN priority field so that it can be managed in VLAN bridging mode. Management traffic is identified with unit VLAN ID and destination MAC address.

Command Syntax:

ip route vlan-priority <0-7>

Set the VLAN Priority field.

Command Mode: Config

Example

ip static-route clear

Use the **ip static-route clear** to clear the static routing table.

Command Syntax:

ip static-route clear

Command Mode: Config

multilink

Use the **multilink** command to enable multilink PPP or multilink Frame Relay and configure the multilink protocol parameters.

Command Syntax:

multilink [yes | no

yes]

multilink mfr

Use the **multilink mfr** command to configure multilink Frame Relay protocol parameters.

Command Syntax:

link-ack [1-10]

link-integrity-timer [1-180]

retry-counter [1-5]

multilink mlppp

Use the **multilink mlppp** command to configure multilink PPP protocol parameters.

Command Syntax:

keep-alive-timeout [1-10]

keep-alive-timer [1-180]

retry-counter [1-5]

t1 framing

Use the **t1 framing** command to configure the network T1 framing format.

Command Syntax: t1 framing [net1 | net2] [esf | d4]

Command Mode: Config

Example

unit(config)#t1 framing net1 esf

unit(config)#

t1 lbo

Use the **t1 lbo** command to to set the Line Build Out (LBO) value to be used for tuning the circuit attenuation between the unit and the last repeater on the T1 circuit.
Command Syntax: t1 lbo [0dB | -7.5dB | -15 dB]
Command Mode: Config
Example

t1 timeslot

Use the **t1 timeslot** command to allocate an T1 timeslot and assign it to data, voice or idle.
Command Syntax: t1 timeslot <1-23> [aux | f1 | idle]
<1-31> select an E1 timeslot number
aux Assign selected timeslot to auxiliary dro-and-insert port
f1 Assign selected timeslot to Ethernet data port
idle Selected timeslot will not be used
Command Mode: Config
Example
Assign timeslot 10 to transport data from Ethernet data port.
unit(config)#e1 timeslot 10 f1

time-sync

Use the **time-sync** command to configure the RFC-868 time protocol client.
Command Syntax:
time-sync [enabled | disabled] Enable of disables time synchronization.
time-sync attempt-count [1-30]
time-sync attempt-interval [1-10]
time-sync frequency days [0-99]
time-sync frequency hours [0-23]
time-sync frequency minutes [0-59]
time-sync frequency seconds [0-59]
time sync primary-ip A.B.C.D
time-sync secondary-ip A.B.C.D
time-sync port [enet | net | comm]

time-zone

Use the **time-zone** command to configure the GMT time zone.
Command Syntax:
time-zone ahead-gmt [yes | no]
time-zone day-light-savings [enabled | disabled]
time-zone day-light-savings diff-minutes [0-59]
time-zone day-light-savings start-month [0-12]
time-zone day-light-savings start-week [0-5]
time-zone offset-gmt minutes [0-59]
time-zone day-light-savings diff-hours [0-12]
time-zone offset-gmt hours [0-12]

traffic monitoring

Use the **traffic monitoring** command to enable or disable RMON1 and RMON2 traffic monitoring.
Command Syntax:
traffic monitoring [enabled | disabled]

traffic type

Use the **traffic** command to set the WAN protocol to Frame Relay or PPP.
Command Syntax:
traffic type [frame-relay | ppp]

unit alarm

Use the **unit alarm** command to configure the network alams that will be generated to the NMS.
Command Syntax:
unit alarm inband-lonk-loss [enabled | disabled]
unit alarm interface [net | aux] [carrier-loss | sync-loss | ais-received | yellow-received] [enabled | disabled]
unit alarm interface enet carrier-loss [enabled | disabled]

unit ansi-fdl

Use the **unit ansi-fdl** command to enable or disable standard remote monitoring ansi-fdl.
Command Syntax:
unit ansi-fdl [enabled | disabled]

unit clock

Use the **unit clock** command to configure the primary and secondary clock.
Command Syntax:
unit clock primary [net | net1| net2 | aux | internal]
unit clock secondary [net | net1| net2 | aux | internal]

unit comm-port

Use the **unit comm-port** command to configure the console port and flow control.
mand Syntax:
unit comm-port baud [9600 | 14400 | 19200 | 28800 | 38400]
unit comm-port dcd [enabled | disabled]
unit comm-port parity [none | odd | even]
unit comm-port stop-bits [1 | 2]
unit comm-port word-length [7-8]
unit comm-port xon-xoff [disabled | xoff-until-xon | xoff-unti-any]

unit id

Use the **unit id** command to set the unit identifier
Command Syntax:
unit id [HOSTNAME]

unit idle-code

Use the **unit idle-code** command to set the idle code.
Command Syntax:
unit idle-code [0-ff]

unit management

Use the **unit management** command to configure the dial out management feature.
Command Syntax:
unit management connection [direct | fdl | modem]
unit management connection-timeout-logged-on [unlimited | 1-minute | 10-minutes | 30-minutes]
unit management connection-timeout-not-logged-on [unlimited | 1-minute | 10-minutes | 30-minutes]
unit management dial-out-time [0-255]
unit management phone1 WORD
unit management phone2 WORD

unit modem

Use the **unit monitor-jack** command to set the monitor jack to net 1 or net2.
Command Syntax:
unit modem str1 WORD
unit modem str2 WORD

unit outage

Use the **unit outage** command is reserved to configure outage source event.

unit protect-mode

Use the **unit protect-mode** command to enable or disable changes from front panel.
Command Syntax:
unit protect-mode [enabled | disabled]

unit radius

Use the **unit radius** command to configure RADIUS client.
Command Syntax:
unit radius [primary-server | secondary-server] ip A.B.C.D
unit radius [retries | response-time] [1-3]
unit radius group-id WORD
unit radius protocol [yes | no]

unit remote-comm

Use the **unit remote-comm** command to set the remote communication protocol.
Command Syntax:
unit remote-comm [none | att | ansi]

unit sla

Use the **unit sla** command to configure Frame Relay SLA parameters.
Command Syntax:
unit sla [enabled | disabled]
unit sla [fdr-ddr-sample-period | delay-period] [1-255]
unit sla [fdr | ddr] threshold WORD
unit sla delay-packet-size [50-1500]

unit snmp

Use the **unit snmp** command to configure the SNMP community strings and the three Network Management unit.
Command Syntax:
unit snmp community [get } set | trap] LINE
unit snmp trap [1 | 2 | 3] A.B.C.D
unit snmp trap port [1 | 2 |3] [comm | net1 | net2 | bundle0 | enet]

unit yellow-alarm

Use the **unit yellow-alarm** command to enable or disable yellow alarm
Command Syntax:
unit yellow-alarm [enabled | disabled]

wan-port in-service

Use the **wan-port** command to enable or disable service on the NET1 and NET2 WAN ports.
Command Syntax:
want-port in-service [port1 | port2] [yes | no]

KERNEL COMMAND REFERENCE

Kernel mode lets you access all the routing tables and interfaces and the various routing protocols modes.

interface IFNAME

Use the **interface IFNAME** command to change to configure terminal mode.

Command Syntax: interface [net1 | net2 | mlppp | e0]

The argument to this command is one of the router interface e0 for ethernet port, net1 for PPP1, net2 for PPP2, or bundle0 for multilink

Command Mode: Enable

Usage

There are no arguments or keywords for this command. The prompt will change to

Rip(config)#

Example

```
kernel(enable)#show interface net1
 36: Interface net1
 37:   index 3 metric 1 mtu 1500 <UP,POINTOPOINT,RUNNING>
kernel(enable)#show int net2
 57: Interface net2
 58:   index 4 metric 1 mtu 1500 <UP,POINTOPOINT,RUNNING>
 59:   inet 60.10.2.2/24 pointopoint 60.10.2.1 secondary net2
kernel(enable)#show interface
 39: Interface e0
 40:   index 1 metric 1 mtu 1500 <UP,BROADCAST,RUNNING>
 41:   HWaddr: 00:a0:c0:00:37:86
 42:   inet 172.18.65.10/24 broadcast 255.255.255.255 secondary e0
 43: Interface mlppp
 44:   index 2 metric 1 mtu 1500 <>
 45: Interface net1
 46:   index 3 metric 1 mtu 1500 <UP,POINTOPOINT,RUNNING>
 47: Interface net2
 48:   index 4 metric 1 mtu 1500 <UP,POINTOPOINT,RUNNING>
 49:   inet 60.10.2.2/24 pointopoint 60.10.2.1 secondary net2
```

quit

Use the **quit** command to change exit from the current mode and return to the higher level mode.

Command Syntax: quit

Example

Kernel(config)#**quit**

Kernel(enable)#

debug zebos events

Use the **debug zebos events** command to specify the set of debug options for zebosd events.

Command Syntax: debug zebos events

no debug zebos events

There are no arguments or keywords for this command.

Command Mode: Enable

debug zebos kernel

Use the **debug zebos kernel** command to specify the debug option-set for the zebos routing manager between the kernel interface
Command Syntax: debug zebos kernel
no debug zebos kernel
There are no arguments or keywords for this command.
Command Mode: Enable

debug zebos packet

Use the **debug zebos packet** command to specify the debug option-set for the zebos packet
Command Syntax:
debug zebos packet [recv | send | detail]
no debug zebos packet
recv Specifies the debug option-set for receive packet.
send Specifies the debug option-set for send packet.
detail Sets the debug option set to detailed information.
Command Mode: Enable
Examples:
debug zebra packet
debug zebra packet recv detail

show debugging zebos

Use the **show debugging zebos** command to display debugging information for the zebos routing manager.
Command Syntax
show debugging zebos
Command Mode: Enable
There are no arguments or keywords for this command.
Examples
show debugging zebos

show interface IFNAME

Use the **show nterface** command to display interface configuration and status
Command Syntax: show interface IFNAME
IFNAME specifies the name of the interface for which status and configuration is desired:
net1 for network port 1
net2 for network port 2
bundle0 for multilink bundle 0
e0 for ethernet port
Command Mode: Enable
Example

```
kernel(enable)#show interface mlppp
142:Interface mlppp
143:index 2 metric 1 mtu 1500 <>
kernel(enable)#show interface net1
145:Interface net1
146:index 3 metric 1 mtu 1500 <UP,POINTOPOINT,RUNNING>
147:inet 10.1.1.2/24 pointopoint 10.1.1.1 secondary net1
kernel(enable)#show interface net2
149:Interface net2
150:index 4 metric 1 mtu 1500 <UP,POINTOPOINT,RUNNING>
151:inet 10.1.3.1/24 pointopoint 10.1.3.2 secondary net2
kernel(enable)#show interface e0
156: Interface e0
157:index 1 metric 1 mtu 1500 <UP,BROADCAST,RUNNING>
158:HWaddr: 00:a0:c0:00:4d:3f
```

show ip route

Use the **show ip route** command to display the IP routing table for a protocol or from a particular table.

Command Syntax: show ip route
Command Mode: Enable
connected Connected
kernel Kernel
rip Routing Information Protocol (RIP)
static Static routes
A.B.C.D Network in the IP routing table to display
A.B.C.D/M IP prefix <network>/<length>, e.g., 35.0.0.0/8
Examples

```
kernel(enable)#show ip route
106:Codes: K - kernel route, C - connected, S - static, R - RIP, > - selected route, * - FIB route
108:
109:C>* 10.1.1.0/24 is directly connected, net1
110:S   10.1.1.0/24 [1/0] is directly connected, net1
111:C>* 10.1.3.0/24 is directly connected, net2
112:S   10.1.3.0/24 [1/0] is directly connected, net2
113:S   10.20.30.0/24 [3/0] is directly connected, net2
114:S>  10.20.30.0/24 [2/0] is directly connected, net1
115:S   70.80.90.0/24 [3/0] is directly connected, net1
116:S>  70.80.90.0/24 [2/0] is directly connected, net2
117:C>* 172.30.65.0/24 is directly connected, e0
118:S   172.30.65.0/24 [1/0] is directly connected, e0

kernel(enable)#show ip route rip
90: Codes: K - kernel route, C - connected, S - static, R - RIP,
91:          > - selected route, * - FIB route 92:
93: R>  60.10.1.0/24 [120/2] via 60.10.2.1, net2, 08w5d11h
94: R>  60.10.1.2/32 [120/2] via 60.10.2.1, net2, 08w5d11h
95: R>  60.10.4.0/24 [120/2] via 60.10.2.1, net2, 08w5d11h
96: R>  60.10.4.2/32 [120/2] via 60.10.2.1, net2, 08w5d11h
97: R>  60.10.5.0/24 [120/2] via 60.10.2.1, net2, 08w5d11h
98: R>  172.18.0.0/16 [120/2] via 60.10.2.1, net2, 08w5d11h
```

show running-config

Use the **show running-config** command to show running config.
Command Syntax
show running-config
Command Mode: enable
There are no arguments or keywords for this command.
Examples

```
kernel(enable)#show running-config
76:
77: Current configuration:
78: !
79: hostname router
80: password zebos
81: enable password zebos
82: !
83: interface e0
84:  shutdown
85: !
86: interface mlppp
87:  shutdown
88: !
89: interface net1
90:  shutdown
91: !
92: interface net2
93: !
94: ip route 33.33.0.0/16 net2 0
95: ip route 44.44.0.0/16 net2 0
96: !
97: line vty
98:  no login
99: !
100: end
```

RIP COMMAND REFERENCE

configure terminal

Use the **configure terminal** command to change to configure terminal mode.
Command Syntax: **c**onfigure terminal
Command Mode: Enable
Usage
There are no arguments or keywords for this command. The prompt will change to
Rip(config)#
Example
Rip(enable)#configure terminal
Rip(config)#

router rip

Use the **router rip** command to change to configure router mode.
Command Syntax
router rip
Usage
There are no arguments or keywords for this command. The prompt will change to
Rip(router rip)#
Example
Rip(config)#**router rip**
Rip(rip)#

interface IFNAME

Use the **interface IFNAME** command to change from configure terminal mode to configure interface mode.
Command Syntax: interface net1 | net2 | mlppp | e0
Command Mode:: Config
Usage
The argument to this command is one of the router interface e0 for ethernet port, net1 for PPP1, net2 for PPP2, or mlppp for MLPPP
Example
Rip(config)#**interface net1**
Rip(net1)#

quit

Use the **quit** command to change exit from the current mode and return to the higher level mode.
Command Syntax: quit
Example
Rip(config)#**quit**
Rip(enable)#

debug rip

Use the **debug rip** command to specify the options for the displayed debugging information for RIP events. Use the no parameter to disable all debugging.
Command Syntax
debug rip (events|zebos|packet)
events - RIP events debug information is displayed.
zebos - RIP and ZebOS communication is displayed
packet - packet (recv|send (detail)) Specifies RIP packets only
debug rip packet
recv - specifies that information for received packets be displayed.

send - specifies that information for sent packets be displayed.
no debug rip (events | packet | zebos)
Command Mode:: Enable
Examples
RIP(enable)#debug rip events
7: RECV packet from 60.10.2.1 port 520 on net2
8: update timer fire!
9: SEND UPDATE to net2 ifindex 4
10: unicast announce to 60.10.2.1 on net2
11: update routes to neighbor 60.10.2.1
12: SEND to socket 34 port 520 addr 60.10.2.

distance

Use the **distance** command to set the administrative distance.
Use the **no** form of the command to disable this function.
Command Syntax
(no) distance DISTANCE (A.B.C.D/M (ACCESSLIST))
DISTANCE=<1-255> Specifies the administrative distance value.
A.B.C.D(/M) Specifies the network prefix and length.
ACCESSLIST Specifies the access-list name.
Command Mode:: Router Configuration
Examples
distance 8 10.0.0.0/8 mylist
no distance 9

ip rip receive-packet

Use the **ip rip receive** packet command to configure the interface to enable the reception of RIP packets. This feature allows the user to control the receiving of packets directly on the specified interface. Therefore, the packet receiving is more efficient and controllable.
Command Syntax
ip rip receive-packet
no ip rip receive-packet
Command Mode:: interface
Examples
ip rip receive-packet

ip rip receive version

Use the **ip rip receive version** command to receive specified version of RIP packets on an interface basis using version control, and override the setting of the version command.
Use the no form of this command to use the setting established by the version command.
Command Syntax
ip rip receive version 1|2|[1 2]
no ip rip receive version (1|2|[1 2])
1 - specifies acceptance of RIP version 1 packets on the interface.
2 - specifies acceptance of RIP version 2 packets on the interface.
1 2 - specifies acceptance of RIP version 1 and version 2 packets on the interface.
Command Mode: Router Configuration
Examples
ip rip receive version 1 2
Related Commands
version

ip rip send-packet

Use the **ip rip send** packet command to configure the interface to enable the sending of RIP packets. This feature allows the user to control the sending of packets directly on the specified interface. Therefore, the packet sending is more efficient and controllable.

Command Syntax

ip rip send-packet

no ip rip send-packet

Command Mode: interface

Examples

ip rip send-packet

ip rip send version

Use the **ip rip send version** command to send RIP packets on an interface using version control.

Use the **no** option on this command to use the global RIP version control rules.

Command Syntax

ip rip send version 1|2|[1 2]

no ip rip send version (1|2)

1 - specifies sending of RIP version 1 packets out of an interface.

2 - specifies sending of RIP version 2 packets out of an interface.

1 2- permits sending of both RIP version 1and 2 packets out of an interface.

Command Mode: Router Configuration

Examples

ip rip send version 1

ip rip send version 1-compatible

Use the ip rip send version 1-compatible command to send RIP version 1 compatible packets from a version 2 RIP interface to other RIP interfaces. This mechanism causes version 2 RIP to broadcast the packets instead of multicasting them.

Use the **no** option on this command to use the global RIP version control rules.

Command Syntax

ip rip send version 1-compatible

Command Mode: Router Configuration

Examples

ip rip send version 1-compatible

Usage Notes

For testing this case, the configuration must be:!

interface XXXX

ip rip send version 1-compatible

!

router rip

version 2

NOTE: The default version for ripd is version 2. Use the `version` command to explicitly specify a different version.

ip split-horizon

Use the **ip split-horizon** command to perform the split-horizon action on the interface. The default is `split-horizon poisoned`.

Use the **no** option on this command to disable this function.

Command Syntax

ip split-horizon (poisoned)

`poisoned` perform split-horizon with poisoned reverse.

no ip split-horizon

Command Mode: Router Configuration

Examples

ip split-horizon

neighbor

Use the **neighbor** command to specify a neighbor router. It is used for each connected point-to-point link. Use the no parameter to disable the specific router.

Command Syntax

(no) neighbor A.B.C.D

A.B.C.D is an IP address of a neighboring router with which the routing information will be exchanged.

Command Mode: configuration mode

Examples

neighbor 1.1.1.

network

Use the **network** command to specify a network as one that runs Routing Information Protocol (RIP). Use the no parameter to remove the specified network as one that runs RIP.

Command Syntax

(no) network [A.B.C.D(/M)]|IFNAME

A.B.C.D(/M) - specifies the IP address prefix and length of this IP network.

IFNAME - alphanumeric string specifies the interface name.

Command Mode: Router Configuration

Examples

network 10.0.0.0/8

network eth0

passive-interface

Use the **passive-interface** command to enable suppression of routing updates on an interface.

Use the **no** form of this command to disable this function

Command Syntax

(no) passive-interface IFNAME

IFNAME - specifies the interface name.

Command Mode: Router Configuration

Examples

passive-interface eth0

route

Use the **route** command to configure static RIP routes.

Use the **no** form of the command to disable this function.

Command Syntax

(no) route A.B.C.D/M

A.B.C.D(/M) - specifies the IP address prefix and length

Command Mode: Router Configuration

Examples

route 1.2.3.4/8

Usage

router rip

...

version 1

network 10.10.10.0/24

network 10.10.11.0/24

neighbor 10.10.10.10...

ripd(config-router)# route 10.10.10.0/24...

version 1

network 10.10.10.0/24

network 10.10.11.0/24

route 10.10.10.0/24

router rip

Use the **router rip** global command to enable a RIP routing process.
Use the **no** form of the command to disable the RIP routing process.
(no) router rip
Command Syntax
There are no arguments or keywords for this command.
Command Mode: Router Configuration
Examples
router rip
Usage Notes
router rip
 version 1
 network 10.10.10.0/24
 network 10.10.11.0/24
 neighbor 10.10.10.10

show debugging rip

Use the **show debugging rip** command to display the RIP debugging status for these debugging options:
zebos debugging, RIP event debugging, RIP packet debugging and RIP zebos debugging.
Command Syntax
show debugging rip
Command Mode: Enable
There are no arguments or keywords for this command.
Examples
show debugging rip

show ip protocols

Use the **show ip protocols** command to display RIP process parameters and statistics.
Command Syntax
show ip protocols
Command Mode: Enable
There are no arguments or keywords for this command.
Examples
show ip protocols
RIP(enable)#show ip protocols
 116: Routing Protocol is "rip"
 117: Sending updates every 30 seconds with +/-50%, next due in 14 seconds
 118: Timeout after 180 seconds, garbage collect after 120 seconds
 119: Outgoing update filter list for all interface is not set
 120: Incoming update filter list for all interface is not set
 121: Default redistribution metric is 1
 122: Redistributing: connected
 123: Default version control: send version 2, receive version 2
 124: Interface Send Recv Key-chain
 125: net2 2 2
 126: Routing for Networks:
 127: net1
 128: net2
 129: Routing Information Sources:
 130: Gateway BadPackets BadRoutes Distance Last Update
 131: 60.10.2.1 0 0 120 00:15:22
 132: Distance: (default is 120)

show running-config

Use the **show running-config** command to show running config.

Command Syntax

show running-config

Command Mode: rip

There are no arguments or keywords for this command.

Examples

```
Rip(enable)#show running-config
2:
3: Current configuration:
4: !
5: hostname router
6: password zebos
7: enable password zebos
8: !
9: interface e0
10: !
11: interface mlppp
12: !
13: interface net1
14: !
15: interface net2
16: !
17: router rip
18:  redistribute connected
19:  network net1
20:  network net2
21: !
22: line vty
23:  no login
24: !
25: end
Rip(enable)#
```

show ip rip

Use the **show ip rip** command to show RIP routes.

Command Syntax

show ip rip

Command Mode: Enable

There are no arguments or keywords for this command.

Examples

show ip rip

```
RIP(enable)#show ip rip
104: Codes: R - RIP, C - connected, O - OSPF, B - BGP
105:
106:    Network          Next Hop        Metric From          Time
107: R  60.10.1.0/24     60.10.2.1            2 60.10.2.1     42:45
108: R  60.10.1.2/32     60.10.2.1            2 60.10.2.1     42:45
109: C  60.10.2.0/24                          1
110: R  60.10.4.0/24     60.10.2.1            2 60.10.2.1     42:45
111: R  60.10.4.2/32     60.10.2.1            2 60.10.2.1     42:45
112: R  60.10.5.0/24     60.10.2.1            2 60.10.2.1     42:45
113: R  172.18.0.0/16    60.10.2.1            2 60.10.2.1     42:45
114: C  172.18.65.0/24                        1
```

timers

Use the **timers** command to adjust routing network timers.

Use the **no** form of the command to restore the defaults.

Command Syntax

timers basic TABLETIMER INFORMATIONTIMER GARBAGETIMER

no timers basic

TABLETIMER=<0-4294967295> Specifies the routing table update timer in seconds. The default is 30 seconds.

INFORMATIONTIMER=<0-4294967295> Specifies the routing information timeout timer in seconds. The default is 180 seconds. After this interval has elapsed and no updates for a route are received, the route is declared invalid.

GARBAGETIMER=<0-4294967295> Specifies the routing garbage collection timer in seconds. The default is 120 seconds.
Command Mode: Router Configuration
Examples
timers 30 180 120

version

Use the **version** command to set a RIP routing protocol version.
Use the **no** form of the command to restore the default.
Command Syntax
version <1-2>
no version <1-2>
<1-2> - specifies the version of RIP processing. Default is RIP v2.
Command Mode: Router Configuration
Examples
version 1
Usage
ripd# sh run...
router rip
network 10.10.10.0/24
network 10.10.11.0/24
ripd(config-router)# version 1
router rip...
version 1
network 10.10.10.0/24
network 10.10.11.0/24

OSPF COMMAND REFERENCE

area authentication

Use the area authentication command to enable authentication for an OSPF area. Use the no parameter to remove the authentication specification for an area.
Command Syntax
area AREAID authentication
no area AREAID authentication
AREAID= A.B.C.D|<0-4294967295>
A.B.C.D= The IPv4 specification of the area for which to enable authentication.
<0-4294967295>= The area identification number of the area for which to enable authentication.
Default
Type 0 authentication or no authentication.
Command Mode: Router mode
Usage
Specifying the area authentication sets the authentication to Type 1 authentication or the Simple Password authentication (details in RFC 2328). Setting up a Type 1 authentication configures a 64-bit field for that particular network. All packets sent on this network must have this configured value in their OSPF header. This allows only routers that have the same passwords to join the routing domain. Give all routers that are to communicate with each other through OSPF the same authentication password.
Use the ip ospf authentication-key command to specify an OSPF authentication password.
Examples
ospfd# configure terminal
ospfd(config)# router ospf 100
ospfd(config-router)# area 1 authentication

Related Commands
area default-cost, area stub, ip ospf authentication-key

area default-cost

Use the area default-cost command to specify a cost for the default summary route sent into a stub.
Use the no form of this command to remove the assigned default-route cost.
Command Syntax
area AREAID default-cost <0-16777215>
no area AREAID default-cost
AREAID=A.B.C.D|<0-4294967295>
A.B.C.D= The IPv4 specification of the address for the stub.
AREAADDRESSID= The area identification number for the stub.
default-cost Indicates the cost for the default summary route used for a stub. Default value of cost is 1.
Command Mode: Router mode
Usage
Area command has two configuration options, stub and default-cost. The default-cost option provides the metric for the summary default route, generated by the area border router, into the stub area. Use this option only on an area border router that is attached to the stub area. Refer to RFC 1587 for information on stub area.
Examples
This example sets the default-cost to 10 for area 1.
ospfd# configure terminal
ospfd(config)# router ospf 100
ospfd(config-router)# area 1 default-cost 10
Related Commands
area authentication, area stub

area export-list

Use the area export-list command to define restrictions on routes that are advertised from a specified area.
Use the no form of this command to disable this function.
Command Syntax
area AREAID export-list NAME
no area AREAID export-list
AREAID=A.B.C.D|<0-4294967295>
A.B.C.D= The IPv4 specification of the address for the stub.
<0-4294967295>= The area identification number for the stub.
NAME The name of the configured access list.
Command Mode: Router mode
Usage
Use the export-list in combination with the access list to specify the routes that will be advertised to other areas.This command is applied only when generating summary-LSAs (type 3).
Examples
ospfd# configure terminal
ospfd(config)# access-list list1 deny 172.22.0.0/8
ospfd(config-router)# area 1 export-list list1
Related Commands
access list

area import-list

Use the area import-list command to import summary routes from a stub.
Use the no form of this command to disable this function.
Command Syntax
area AREAID import-list NAME
no area AREAID import-list

AREAID=A.B.C.D|<0-4294967295>
A.B.C.D= The IPv4 specification of the address for the stub.
<0-4294967295>= The area identification number for the stub.
NAME The name of the configured access list.
Command Mode: Router mode
Usage
In conjunction with IP access list, this command is used to configure routes outside the area that will be advertised into this area. This command is only applied when generating summary LSAs (type 3).
Examples
ospfd# configure terminal
ospfd(config)# access-list list1 deny 172.22.0.0/8
ospfd(config)# router ospf 100
ospfd(config-router)#area 1 import-list list1
Related Commands
access list

area range

Use the area range command to summarize OSPF routes at an area boundary.
Use the no form of this command to disable this function.
Command Syntax
area AREAID range ADDRESS (advertise|not-advertise|SUBSTITUTE)
no area AREAID range
AREAID= A.B.C.D|<0-4294967295>
A.B.C.D= The IPv4 address specification of the address for the stub.
<0-4294967295>= The area identification number for the stub.
ADDRESS= A.B.C.D/M The area range prefix and length.
advertise Advertises this range.
not-advertise Does not advertise this range.
SUBSTITUTE = substitute A.B.C.D/M Announce area range as another prefix.
A.B.C.D/M = Network prefix to be announced instead of range.
Default
Disabled
Command Mode
Router mode
Usage
The area range command is used to summarize intra-area routes for an area. The single summary route is then advertised to other areas by the Area Border Routers (ABRs). Routing information is condensed at area boundaries and outside the area. If the network numbers in an area are assigned in a way such that they are contiguous, the ABRs can be configured to advertise a summary route that covers all the individual networks within the area that fall into the specified range.
Examples
ospfd# configure terminal
ospfd(config)# router ospf 100
ospfd(config-router)# area 1 range 192.16.0.0/24
Related Commands

area shortcut

Use the area shortcut command to configure the short-cutting mode of an area.
Use the no form of this command to disable this function.
Command Syntax
area AREAID shortcut (default|enable|disable)
no area AREAID shortcut (enable|disable)
AREAID= A.B.C.D|<0-4294967295>
A.B.C.D= The IPv4 address specification of the address for the stub.

<0-4294967295>= The area identification number for the stub.
default Sets default short-cutting behavior.
enable Forces short-cutting through the area.
disable Disables short-cutting through the area.
Default
Command Mode
Router mode
Usage
Examples
area 1 shortcut default
area 52 shortcut disable
no area 42 shortcut enable
Related Commands
ospf abr-type shortcut

area stub

Use the area stub command to define an area as a stub area.
Use the no form of this command to disable this function.
Command Syntax
(no) area AREAID stub (no-summary)
AREAID= A.B.C.D|<0-4294967295>
A.B.C.D= The IPv4 address specification of the identifier for the stub.
<0-4294967295>= The area identification number for the stub.
no-summary Stops an ABR from sending summary link advertisements into the stub area.
Default
No stub area is defined.
Command Mode
Router mode
Usage
Configures the area stub command on all routers in the stub area. There are two stub area router configuration commands: the stub and default-cost commands. In all routers attached to the stub area, configure the area by using the stub option of the area command. For an area border router (ABR) attached to the stub area, use the areadefault-cost command.
Examples
ospfd# configure terminal
ospfd(config)# router ospf 100
ospfd(config-router)# area 1 stub
Related Commands
area authentication, area default-cost

area virtual-link

Use the area virtual-link command to configure a link between a non-backbone area that cannot be physically connected to the backbone area, through another non-backbone area. Use the no form of this command to remove a virtual link.
Command Syntax
(no) area AREAID virtual-link A.B.C.D (AUTHENTICATION|AUTHKEY|INTERVAL)
AREAID=A.B.C.D|<0-4294967295>
A.B.C.D= OSPF area ID in IP address format.
<0-4294967295>= range of the number of the OSPF area to be linked.
A.B.C.D = The IP address associated with a virtual link neighbor.
AUTHENTICATION = authentication (|null|AUTHKEY)
authentication= Enable authentication on this virtual link
null = Use null authentication to override password or message digest.
AUTHKEY = authentication-key KEY
KEY = An 8 character password

INTERVAL=dead-interval|hello-interval|retransmit-interval|transmit-delay VALUE
VALUE = <1-65535> The number of seconds in the delay or interval.
hello-interval= The interval the router waits before it sends a hello packet. The default is ten seconds.
retransmit-interval= The interval the router waits before it retransmits a packet. The default is five seconds.
transmit-delay= The interval the router waits before it transmits a packet.The default value is one second.
dead-interval= The interval during which no packets are received and after which the router considers a neighboring router as off-line. The default is 40 seconds.

Command Mode

Router mode.

Usage

In OSPF, all non-backbone areas must be connected to a backbone area. If the connection to the backbone is lost, the virtual link repairs the connection.
You can configure virtual links between any two backbone routers that have an interface to a common non-backbone area. The protocol treats these two routers joined by a virtual link as if they were connected by an unnumbered point-to-point network.To configure virtual link, include both the transit area ID and the corresponding virtual link neighbor's router ID in the virtual link neighbor. To see the router ID use the show ip ospf command.
Configure the Hello-interval to be the same for all routers attached to a common network. If the hello-interval is short, the router detects topological changes faster, but more routing traffic follows. Retransmit-interval is the expected round-trip delay between any two routers in a network. Set the value to be greater than the expected round-trip delay to avoid needless retransmissions.
Transmit-delay is the time taken to transmit a link state update packet on the interface.Before transmission, the link state advertisements in the update packet, are incremented by this amount. Set the transmit-delay to be greater than zero. Also, take into account the transmission and propagation delays for the interface.
Include the transit area ID and the corresponding virtual link neighbor's router ID in each virtual link neighbor to properly configure a virtual link.

Examples (note some examples show abbreviated parameters)

area 123.123.123.1 virtual-link 123.123.123.2
area 123.123.123.1 virtual-link 123.123.123.2 authentication
area 1 virtual-link 123.123.123.2 authentication null
area 1 virtual-link 1.1.1.1 hel 1 ret 2 tran 3 dead 4

Related Commands

area authentication, service password-encryption, show ip ospf

auto-cost

Use the auto-cost command to control how OSPF calculates default metrics for the interface.
Use the no form of this command to assign cost, based only on the interface type.

Command Syntax

auto-cost reference-bandwidth <1-4294967>
no auto-cost reference-bandwidth
<1-4294967> The reference bandwidth in terms of Mbits per second. The default reference bandwidth is 100 Mbps.

Command Mode

Router mode

Usage

By default OSPF calculates the OSPF metric for an interface by dividing the reference bandwidth by the interface bandwidth. The default value for the reference bandwidth is 100Mbps. The auto-cost command is used to differentiate high bandwidth links. For multiple links with high bandwidth, specify a larger reference bandwidth value to differentiate cost on those links.

Examples

ospfd# configure terminal
ospfd(config)# router ospf 100
ospfd(config-router)# auto-cost reference-bandwidth 50

Related Commands

ip ospf cost

compatible rfc1583

Use the compatible rfc1583 command to restore the method used to calculate summary route costs per RFC.
Use the no form of this command to disable RFC 1583 compatibility.

Command Syntax

(no) compatible rfc1583

Default

By default, OSPF is rfc 2328 compatible.

Command Mode

Router mode

Usage

Prior to RFC 2328, OSPF was compliant with RFC 1583, that specified method for calculating the metric for summary routes based on the minimum metric of the component paths available. RFC 2328 specifies a method for calculating metrics based on maximum cost. With this change, it is possible that all of the ABRs in an area might not be upgraded to the new code at the same time. Compatible rfc1583 command addresses this issue and allows the selective disabling of compatibility with RFC 2328.

Examples

ospfd# configure terminal
ospfd(config)# router ospf 100
ospfd(config-router)# compatible rfc1583

Related Commands

debug ospf event

Use the debug ospf event command to specify debugging options for OSPF event troubleshooting. Use this command without parameters to turn on all the options.
Use the no form of this command to disable this function.

Command Syntax

(no) debug ospf event (abr|asbr|lsa|os|router|vl)
abr shows ABR events
asbr shows ASBR events
lsa shows LSA events
os shows OS interaction events
router shows other router events
vl shows virtual link events

Command Mode

Privileged EXEC mode and Configure mode

Usage

Examples

ospfd# no debug ospf event abr
ospfd# debug ospf event asbr
ospfd# debug ospf event lsa
ospfd# debug ospf event os
ospfd# debug ospf event router
ospfd# debug ospf event vl

Related Commands

terminal monitor, log file

debug ospf ism

Use the debug ospf ism command to specify debugging options for OSPF Interface State Machine (ISM) troubleshooting.
Use the no form of this command to disable this function.

Command Syntax

(no) debug ospf ism (status|events|timers)
events Displays ISM event information
status Displays ISM status information

timers Displays ISM timer information
Command Mode
Privileged EXEC mode and Configure mode
Usage
Examples
ospfd# no debug ospf ism events
ospfd# debug ospf ism status
ospfd# debug ospf ism timers
Related Commands
terminal monitor, log file

debug ospf lsa

Use the debug ospf lsa command to specify debugging options for OSPF Link State Advertisements (LSA) troubleshooting.
Use the no form of this option to disable this function.
Command Syntax
(no) debug ospf lsa (generate|flooding|install|maxagerefresh)
generate Displays LSA generation.
flooding Displays LSA flooding.
install Show LSA installation.
maxage Shows maximum age of the LSA in seconds.
refresh Displays LSA refresh.
Command Mode
Privileged EXEC mode and Configure mode
Usage
Each LSA has an Age field which is incremented every second. LSAs are discarded when the LS Age reaches 3600 i.e.if MaxAge is 3600 seconds (an hour).
Examples
ospfd# no debug ospf lsa refresh
ospfd# debug ospf lsa flooding
ospfd# debug ospf lsa install
ospfd# debug ospf lsa maxage
ospfd# debug ospf lsa generate
Related Commands
terminal monitor, log file

debug ospf nsm

Use the debug ospf nsm command to specify debugging options for OSPF Neighbor State Machines (NSMs).
Use the no option to disable this function.
Command Syntax
(no) debug ospf nsm (status|events|timers)
status Displays NSM status information.
events Displays NSM event information.
timers Displays NSM timer information.
Default
Command Mode
Privileged EXEC mode Configure mode
Usage
Examples
ospfd# debug ospf nsm events
ospfd# no debug ospf nsm timers
Related Commands
terminal monitor, log file

debug ospf packet

Use the debug ospf packet command to specify debugging options for OSPF packets.

Command Syntax

(no) debug ospf packet PARAMETERS (send|recv) (detail)

PARAMETERS = all|dd|hello|ls-request|ls-update|ls-ack

all Specifies debugging for all OSPF packets.

dd Specifies debugging for OSPF database descriptions.

hello Specifies debugging for OSPF hello packets.

ls-ack Specifies debugging for OSPF link state acknowledgments.

ls-request Specifies debugging for OSPF link state requests.

ls-update Specifies debugging for OSPF link state updates.

send Specifies the debug option set for sent packets.

recv Specifies the debug option set for received packets.

detail Sets the debug option set to detailed information.

Command Mode

Privileged EXEC mode and Configure mode

Usage

Examples

ospfd# debug ospf packet all detail

ospfd# debug ospf packet dd send detail

ospfd# no debug ospf packet ls-request recv detail

Related Commands

terminal monitor, log file

debug ospf route

Use the debug ospf route command to specify which route calculation to debug. Use this command without parameters to turn on all the options.

Command Syntax

(no) debug ospf route (ase|ia|install|spf)

ia specifies the debugging of Inter-Area route calculation

ase specifies the debugging of external route calculation

install specifies the debugging of route installation

spf specifies the debugging of SPF calculation

Command Mode

Priviledge Exec mode Configure mode

Usage

Examples

ospfd# debug ospf route

ospfd# no debug ospf route ia

ospfd# debug ospf route install

Related Commands

debug ospf zebos

Use the debug ospf zebos command to specify debugging options for OSPF ZebOS information.

Command Syntax

(no) debug ospf zebos (interface|redistribute)

interface Specifies the zebos interface.

redistribute Specifies zebos redistribute.

Command Mode

Privileged EXEC mode and Configure mode

Usage

Examples

ospfd# debug ospf zebos interface

ospfd# no debug ospf zebos redistribute

Related Commands

terminal monitor, log file

default-information originate

Use the default-information originate command to create a default external route into an OSPF routing domain.

Use the no form of this command to disable this feature.

Command Syntax

default-information originate (ALWAYS|METRIC|ROUTE)

no default-information originate

ALWAYS = always (METRIC|ROUTE) Used to advertise the default route regardless of whether the software has a default route.

METRIC = [METRIC METRIC-TYPE]|[METRIC-TYPE METRIC]

METRIC= metric <1-16777214> (ROUTE)

metric Sets the OSPF metric used in creating the default route. The default metric value is 10. The value used is specific to the protocol.

METRIC-TYPE= metric-type 1|2 (ROUTE)

metric-type Sets the OSPF external link type for default routes.

1 Sets OSPF External Type 1 metrics.

2 Sets OSPF External Type 2 metrics.

ROUTE= route-map WORD

WORD= Specifies the name of route-map.

Command Mode

Router mode

Usage

The system acts like an Autonomous System Boundary Router (ASBR) when you use the default-informationoriginate command to redistribute routes into an OSPF routing domain. An ASBR does not by default, generate a default route into the OSPF routing domain.

When you use the default-information originate command, also specify the route-map map-name option to avoid a dependency on the default network in the routing table.

The metric-type is an external link type associated with the default route advertised into the OSPF routing domain. The value of the external route could be either Type 1 or 2; the default is the Type 2.

Examples

ospfd# configure terminal

ospfd(config)# router ospf 100

ospfd(config-router)# default-information originate always metric 23 metric-type 2 route-map myinfo

Related Commands

default-metric

Use the default-metric command to set default metric values for the OSPF routing protocol.

Use the no form of this command to return to the default state.

Command Syntax

default-metric <1-16777214>

no default-metric

<1-16777214> Default metric value appropriate for the specified routing protocol.

Default

Built-in, automatic metric translations, as appropriate for each routing protocol.

Command Mode

Router mode

Usage

A default metric facilitates redistributing routes even with incompatible metrics. If the metrics do not convert, the default metric provides an alternative and enables the redistribution to continue. Default-metric command is used to cause the current routing

protocol to use the same metric value for all redistributed routes. Use this command in conjunction with the redistribute command.

Examples

ospfd# configure terminal
ospfd(config)# router ospf 100
ospfd(config-router)# default-metric 100

Related commands

redistribute

description

Use the description command to add a description to an interface.
Use the no form of this command to remove the description.

Command Syntax

description LINE
no description
LINE 1-1023 characters that are a description of the ZebOS interface.

Command Mode

Interface mode

Usage

Examples

ospfd# configure terminal
ospfd(config)# interface eth0
ospfd(config-if)# description This interface is ethernet interface

Related Commands

distance

Use the distance command to define OSPF route administrative distances based on route type.
Use the no form of this command to restore the default value.

Command Syntax

distance <1-255>|ROUTEPARAMETER
no distance ospf
<1-255> = OSPF administrative distance.
ROUTEPARAMETER= ospf ROUTE1|ROUTE2|ROUTE3 DISTANCE
ROUTE1= external Sets the distance for routes from other routing domains, learned by redistribution.
ROUTE2= inter-area Sets the distance for all routes from one area to another area.
ROUTE3= intra-area Sets the distance for all routes within an area.
DISTANCE= <1-255> Distance for external, intra-area, or inter-area routes.
Note: Include ROUTE1, ROUTE2 and ROUTE3 parameters one time each in a single command in any order.

Default

The default distance for each type of route (intra, inter or external) is 110.

Command Mode

Router mode

Usage

The administrative distance rates the trustworthiness of a routing information source. The distance could be any integer from 0 to 255. A higher distance value indicates a lower trust rating. For example, an administrative distance of 255 indicates that the routing information source cannot be trusted and should be ignored.
Use this command to set the distance for an entire group of routes, rather than a specific route that passes an access list.

Examples

ospfd# configure terminal
ospfd(config)# router ospf 100
ospfd(config-router)# distance ospf inter-area 20 intra-area 10 external 40

Related Commands

distribute-list

Use the distribute-list command to filter networks in routing updates.
Use the no form of this command to disable this function
Command Syntax
distribute-list LISTNAME out ROUTE
no distribute-list LISTNAME
LISTNAME Specifies the name of the access list.
out Indicates that outgoing advertised routes will be cleared.
ROUTE= kernel | connected | static | rip | ospf | bgp
kernel Specifies kernel routes.
connected Specifies connected routes.
static Specifies static routes.
rip Specifies RIP routes.
ospf Specifies OSPF routes.
Command Mode
Router mode
Usage
Use this command when redistributing other routing protocols into the OSPF routing table.
Examples
The following example shows the distribution of BGP routing updates based on the access list list1 (network 172.10.0.0).
ospfd# configure terminal
ospfd(config)# access-list list1 permit 172.10.0.0 0.0.255.255
ospfd(config)#router ospf 100
ospfd(config-router)# distribute-list list1 out bgp
ospfd(config-router)# redistribute bgp
Related Commands

ip ospf authentication

Use the ip ospf authentication command to send and receive OSPF packets with the specified authentication method.
Use the no form of this command to disable the authentication.
Command Syntax
ip ospf authentication (A.B.C.D|MESSAGE|NULL)
no ip ospf authentication
A.B.C.D = The IP address of the interface.
NULL = null (A.B.C.D) Use no authentication; it overrides password authentication of the interface.
Command Mode
Interface mode
Usage
Examples
ip ospf authentication null
Related Commands
ip ospf authentication-key

ip ospf authentication-key

Use the ip ospf authentication-key command to specify an OSPF authentication password for the neighboring routers.
Use the no form of this command to remove an OSPF authentication password.
Command Syntax
ip ospf authentication-key AUTHKEY (A.B.C.D)
no ip ospf authentication-key (A.B.C.D)
AUTHKEY = Specifies the authentication password. Any continuous string of characters (not more than 8 bytes)
A.B.C.D = IP address of the interface
Default

Authentication password not specified.

Command Mode

Interface mode

Usage

This command creates a password (key) that is inserted into the OSPF header when ZebOS software originates routing protocol packets. Assign a separate password to each network for different interfaces. All neighboring routers on the same network with the same password exchange OSPF routing data.

The key can be used only when authentication is enabled for an area. Use the area authentication command to enable authentication.

Simple password authentication allows a password to be configured for each area. Configure the routers in the same routing domain with the same password.

Examples

ip ospf authentication-key 123

Equivalent Commands

ospf authentication-key, area authentication

ip ospf cost

Use the ip ospf cost command to explicitly specify the cost of sending a packet on an interface.

Use the no form of this command to reset the path cost to the default value.

Command Syntax

ip ospf cost COST (A.B.C.D)

no ip ospf cost (A.B.C.D)

COST = <1-65535> Specifies the link-state metric.The default value is 10.

A.B.C.D = IP address of the interface

Command Mode

Interface mode

Usage

The interface cost indicates the overhead required to send packets across a certain interface. It is inversely proportional to the bandwidth of that interface. By default, the cost of an interface is calculated based on the bandwidth (108/ bandwidth); use this ip ospf cost command to set the cost manually.

Examples

The following example shows setting ospf cost as 10 on interface fxp0 for IP address 10.10.10.50

ospfd# configure terminal

ospfd(config)# interface fxp0

ospfd(config-if)# ip ospf cost 10 10.10.10.50ip ospf cost 123

Related Commands

show ip ospf interface

Equivalent Commands

ospf cost

ip ospf database-filter

This command turns on the LSA database-filter for a particular interface. Use the no parameter to turn off the filter.

Command Syntax

ip ospf database-filter ALL OUT (A.B.C.D)

no ip ospf database-filter (A.B.C.D)

ALL = Filter all LSAs

OUT = Outgoing LSAs

A.B.C.D = IP address of the interface.

Default

Disabled, all outgoing LSAs are flooded to the interface.

Command Mode

Interface mode

Usage

OSPF floods new LSAs over all interfaces in an area, except the interface on which the LSA arrives. This redundancy ensures robust flooding. However, too much redundancy can waste bandwidth and might lead to excessive link and CPU usage in certain topologies, resulting in destabilizing the network. To avoid this, use the database-filter command to block flooding of LSAs over specified interfaces.

Examples

ospfd# configure terminal
ospfd(config)# interface eth0
ospfd(config-if)# ip ospf database-filter all out

Related Commands

ip ospf dead-interval

Use the ip ospf dead-interval command to set the interval during which no hello packets are received and after which a neighbor is declared dead.

Use the no form of this command to return to the default time.

Command Syntax

ip ospf dead-interval INTERVAL (A.B.C.D)
no ip ospf dead-interval (A.B.C.D)
INTERVAL= <1-65535> Specifies the interval in seconds. The default interval is 40 seconds.

Command Mode

Interface mode

Usage

The dead-interval is the amount of time that the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down. This value is advertised in the router's hello packets. It must be a multiple of hello-interval and be the same for all routers on a specific network.

Examples

The following example shows configuring dead-interval for 10 seconds on fxp0 interface for IP address 10.10.10.50.
ospfd# configure terminal
ospfd(config)# interface fxp0
ospfd(config-if)# ip ospf dead-interval 10 10.10.10.50

Related Commands

ip ospf hello-interval, show ip ospf interface
Equivalent Commands
ospf dead-interval

ip ospf hello-interval

Use the ip ospf hello-interval command to specify the interval between hello packets.

Use the no form of this command to return to the default time.

Command Syntax

ip ospf hello-interval INTERVAL (A.B.C.D)
no ip ospf hello-interval (A.B.C.D)
INTERVAL= <1-65535> Specifies the interval in seconds. The default interval is 10 seconds.
A.B.C.D = IP address of the interface.

Command Mode

Interface mode

Usage

The hello-interval is advertised in the hello packets. Configure the same hello-interval for all routers on a specific network. A shorter hello interval ensures faster detection of topological changes but results in more routing traffic.

Examples

The following example shows setting the hello-interval for 3 seconds on interface fxp0 for IP address 10.10.10.50.
ospfd# configure terminal
ospfd(config)# interface fxp0
ospfd(config-if)# ip ospf hello-interval 3 10.10.10.50

Related Commands

ip ospf dead-interval, show ip ospf interface
Equivalent Commands
ospf hello-interval

ip ospf network

Use the ip ospf network command to configure the OSPF network type to a type different from the default for the media.
Use the no form of this command to return to the default value.

Command Syntax

ip ospf network broadcast|non-broadcast|point-to-point|point-to-multipoint
no ip ospf network
broadcast Sets the network type to broadcast.
non-broadcast Sets the network type to NBMA.
point-to-multipoint Sets the network type to point-to-multipoint.
point-to-point Sets the network type to point-to-point.

Default

Broadcast type.

Command Mode

interface mode

Usage

Use the ip ospf network command to configure Broadcast Networks as Nonbroadcast Multiaccess Networks (NBMA) and vice versa. You would need to do this if you have routers in your network that do not support multicast addressing.
This command saves you from having to configure neighbors. Configuring NBMA networks requires a fully meshed network or a virtual circuit connecting every router. In case the network is not fully meshed, configure the OSPF network type as a point-to-multipoint network. Routing between two routers that are not directly connected will go through a third router that has virtual circuits to both routers.

Examples

The following example shows setting the network to point-to-point type on the fxp0 interface.
ospfd# configure terminal
ospfd(config)# interface fxp0
ospfd(config-if)# ip ospf network point-to-point

Equivalent Commands

ospf network

ip ospf priority

Use the ip ospf priority command to set the router priority to determine the designated router for the network.
Use the no form of this command to return to the default value.

Command Syntax

ip ospf priority <1-255> (A.B.C.D)
no ip ospf priority (A.B.C.D)
A.B.C.D = IP address of the interface.

Default

The default priority is 1.

Command Mode

Interface mode

Usage

Set the priority to help determine the OSPF Designated Router (DR) for a network. If two routers attempt to become the DR, the router with the higher router priority becomes the DR. If the router priority is the same for two routers, the router with the higher router ID takes precedence.
Only routers with nonzero router priority values are eligible to become the designated or backup designated router.
Configure router priority for multiaccess networks only and not for point-to-point networks.

Examples

The following example shows setting the OSPF priority value to 3 on the fxp0 interface for the IP address 10.10.10.50.
ospfd# configure terminal

ospfd(config)# interface fxp0
ospfd(config-if)# ip ospf priority 3 10.10.10.50
Related Commands
ip ospf network, neighbor
Equivalent Commands
ospf priority

ip ospf retransmit-interval

Use the ip ospf retransmit-internal command to specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface.
Use the no form of this command to return to the default value.
Command Syntax
ip ospf retransmit-interval INTERVAL (A.B.C.D)
no ip ospf retransmit-interval (A.B.C.D)
INTERVAL= <3-65535> Specifies the time in seconds between retransmissions. Default interval value is 5 seconds.
A.B.C.D = IP address of the interface.
Command Mode
Interface mode
Usage
After sending an LSA to a neighbor, the router keeps the LSA until it receives an acknowledgement. In case the router does not receive an acknowledgement during the set time (the retransmit interval value) it retransmits the LSA.
Set the retransmission interval value conservatively to avoid needless retransmission. The interval should be greater than the expected round-trip delay between two routers.
Examples
The following example shows setting the ospf retransmit interval to 6 seconds on the fxp0 interface for IP address 10.10.10.50.
ospfd# configure terminal
ospfd(config)# interface fxp0
ospfd(config-if)# ip ospf ospf retransmit-interval 6 10.10.10.50
Related Commands

ip ospf transmit-delay

Use the ip ospf transmit-delay command to set the estimated time it takes to transmit a link-state-update packet on the interface.
Use the no form of this command to return to the default value.
Command Syntax
ip ospf transmit-delay DELAY (A.B.C.D)
no ip ospf transmit-delay (A.B.C.D)
DELAY= <1-65535> Specifies the time taken, in seconds, to transmit a link-state-update. The default transmit delay value is 1 second.
A.B.C.D = IP address of the interface.
Command Mode
Interface mode
Usage
The transmit delay value adds a specified time to the age field of an update. If the delay is not added, the time in which the LSA transmits over the link is not considered. This command is especially useful for low speed links. Add transmission and propagation delays when setting the transmit delay value.
Examples
The following example shows setting the OSPF transmit delay time to 3 seconds on the fxp0 interface for IP address 10.10.10.50.
ospfd# configure terminal
ospfd(config)# interface fxp0
ospfd(config-if)# ip ospf transmit-delay 3 10.10.10.50
Equivalent Commands
ospf transmit-delay

login

Use this command to set a password prompt, before entering the configuration mode and to enable password checking.

Command Syntax

(no) login

Default

Enabled.

Command Mode

Line mode

Usage

Login is enabled by default. The no login command allows users to connect directly to the Priviledged Exec mode skipping the password verification prompt. After using the no login command if the user changes to login command again, the system uses the password being used earlier, unless the user specifies a password in the configure mode (see the following example).

Example

The following examples show the use of login and no login command. In this example, a password pass is set (in configure mode) before using the login command.

```
!
ospfd# configure terminal
ospfd(config)# line vty
ospfd(config-line)# no login
!
!
ospfd# configure terminal
ospfd#(config)# password pass
ospfd#(config)# line vty
ospfd#(config-line)# login
!
```

Related Commands

match interface

Use the match interface command to define the interface match criterion.

Use the no form of this command to remove the specified match criterion.

Command Syntax

match interface IFNAME

no match interface

IFNAME A string that specifies the interface for matching.

Default

Disabled

Command Mode

Route-map mode

Usage

To set the conditions for redistributing routes from one routing protocol to another, use the match and set route-map configuration commands. The match commands specify the match criteria under which redistribution is allowed for the current route-map. The set commands specify the set redistribution actions to be performed, if the match criteria are met.

If a route does not match the criteria completely, it will not be advertised for outbound route-maps and neither be accepted for inbound route-maps. You can modify the data by configuring a second route-map section with an explicit match specified.

Use the match interface command to match the first hop interface of a route.

Example

```
ospfd# configure terminal
ospfd(config)# route-map mymap1 permit 10
ospfd(config-route-map)# match interface eth0
```

Related Commands

match tag, match route-type external

match metric

Use the match metric command to match the specified metric value. Use the no parameter to turn off the matching.

Command Syntax

(no) match metric METRICVALUE

METRICVALUE = <0-16777216>

Default

Disabled

Command Mode

Route-map mode

Usage

To set the conditions for redistributing routes from one routing protocol to another, use the match and set route-mapconfiguration commands. The match commands specify the match criteria under which redistribution is allowed for the current route-map. The set commands specify the set redistribution actions to be performed, if the match criteria are met.

If a route does not match the criteria completely, it will not be advertised for outbound route maps and neither be accepted for inbound route maps. You can modify the data by configuring a second route-map section and specifying an explicit match.

Some types of LSAs have specific metric values.Use the match metric command to match metric value.

Examples

ospfd# configure terminal

ospfd(config)# route-map mymap1 permit 10

ospfd(config-route-map)# match metric 100

Related Commands

match tag, match route-type external

match route-type external

Use the match route-type external command to match specified external route type. Use the no parameter to turn off the matching.

Command Syntax

(no) match route-type external (type-1 | type-2)

Default

Disabled

Command Mode

Route-map mode

Usage

To set the conditions for redistributing routes from one routing protocol to another, use the match and set route-mapconfiguration commands. The match commands specify the match criteria under which redistribution is allowed for the current route-map. The set commands specify the set redistribution actions to be performed, if the match criteria are met.

If a route does not match the criteria completely, it will not be advertised for outbound route maps and neither be accepted for inbound route maps. You can modify the data by configuring a second route map section and specifying an explicit match.

Use the match route-type external command to match specific external route types. AS-external LSA is either Type-1 or Type-2. External type-1 matches only Type 1 external routes and external type-2 matches only Type 2 external routes.

Examples

ospfd# configure terminal

ospfd(config)# route-map mymap1 permit 10

ospfd(config-route-map)# match route-type external type-1

Related Commands

match tag, match route-type external

match tag

Use the match tag command to match the specified tag value. Use the no parameter to turn off the declaration. Tag is the route tag which is labeled by another routing protocol (BGP or other IGP when redistributing).

Command Syntax

(no) match tag <0-4294967295>

Default

Disabled

Command Mode
Route-map mode
Usage
To set the conditions for redistributing routes from one routing protocol to another, use the match and set route-mapconfiguration commands. The match commands specify the match criteria under which redistribution is allowed for the current route-map. The set commands specify the set redistribution actions to be performed, if the match criteria are met.
If a route does not match the criteria completely, it will not be advertised for outbound route maps and neither be accepted for inbound route maps. You can modify the data by configuring a second route map section with an explicit match specified.
Use the match tag command to match the specified tag value.
Examples
ospfd# configure terminal
ospfd(config)# route-map mymap1 permit 10
ospfd(config-route-map)# match tag 100
Related Commands
match metric, match route-type external

neighbor

Use the neighbor command to configure OSPF routers interconnecting to non-broadcast networks.
Use the no form of this command to remove a configuration.
Command Syntax
(no) neighbor NEIGHBORADDRESS PRIORITY|POLL
NEIGHBORADDRESS=A.B.C.D Specifies the interface IP address of the neighbor.
PRIORITY= priority <0-255> (POLL) Specifies the 8-bit number indicating the router priority value of the non-broadcast neighbor associated with the IP address specified. The default is 0. This keyword does not apply to point-to-multipoint interfaces.
POLL= poll-interval <1-65535> Dead neighbor polling interval in seconds. It is recommended to set this value much higher than the hello interval. The default is 120 seconds.
Command Mode
Router mode
Usage
Configure a router as a broadcast network at the OSPF level. To do this, use the neighbor command and include one neighbor entry for each known nonbroadcast network neighbor. Configure the neighbor address on the primary address of the interface. Poll interval is the reduced rate at which routers continue to send hello packets, when a neighboring router has become inactive. Set the poll interval to be much larger than hello interval (RFC 1247).
Examples
This example shows neighbor configured with a priority value and poll interval time.
ospfd# configure terminal
ospfd(config)# router ospf 100
ospfd(config-router)# neighbor 1.2.3.4 priority 1 poll-interval 90
Related Commands

network area

Use the network area command to define the interfaces on which OSPF runs and to define the area ID for those interfaces.
Use the no form of this command to disable OSPF routing for interfaces defined with the address wildcard-mask pair.
Command Syntax
network AREAADDRESS/M area AREAID
no network
AREAADDRESS=A.B.C.D Specifies the network prefix covered by AREAID.
M Specifies the IP-address-type mask that includes "don't care" bits.
AREAID= A.B.C.D.|<0-4294967295> Specifies the area that is to be associated with the OSPF address range. The area ID can be either a decimal value or an IP address.
Default
Disabled.

Command Mode
Router mode
Usage
The address and mask define interfaces to be associated with a specific OSPF area. The primary address of the interface should be covered by the network area command. Covering only the secondary address does not enable OSPF over that interface.
The mask is used as a shortcut and it helps putting a list of interfaces in the same area. The mask contains wild card bits where 0 is a match and 1 is a don't care bit. For example, 0.0.0.255 is a match in the first three bytes of the network number.
Any individual interface can only be attached to a single area. If the address ranges specified for the different areas overlap, the software will adopt the first area in the network command list and ignore the subsequent overlapping portions.
Specify address ranges that do not overlap.
Examples
ospfd# configure terminal
ospfd(config)# router ospf 100
ospfd(config-router)# network 10.0.0.0/8 area 3
ospfd(config-router)# network 10.0.0.0/8 area 1.1.1.1
Related commands

opaque

Use the opaque command to redistribute the specified scope of opaque-LSAs.
Command Syntax
opaque (link|area|as) WORD TYPE ID DATA
link flood opaque-LSA to link-local scope. i.e. the LSA is not flooded over any routers.
area flood opaque-LSA to single area. i.e. the routers in the same area should have the LSAs.
as flood opaque-LSA to whole AS. i.e. the routers in the single AS should have those LSAs.
WORD = if scope is link, WORD is an interface address.
if scope is area, WORD is an Area-ID.
if scope is as, WORD should be ignored.
TYPE = <0-256> Opaque type which is maintained by IANA.
ID = <0-16777216> Opaque ID which is the value specific to the Opaque type.
DATA = Actual Opaque Information which is stored into packet body of Opaque LSAs.
Default
Command Mode
Router mode
Usage
Examples
ospfd# configure terminal
ospfd(config)# router ospf 100
ospfd(config-router)# opaque link mylink 128 65535 mylink
Related Commands

opaque-lsa-capable

Use the opaque-lsa-capable command to enable opaque-lsa; use the no parameter to disable it.
Command Syntax
(no) opaque-lsa-capable
Default
Enabled
Command Mode
Router mode
Usage
Opaque-LSAs are Type 9, 10 and 11 LSAs that deliver information used by external applications.
When using this command, restart the OSPF router.
Examples
ospfd# configure terminal

ospfd(config)# router ospf 100
ospfd(config-router)# opaque-lsa-capable
Related commands

ospf abr-type

Use the ospf abr-type command to set an OSPF area border router (ABR) type.
Use the no parameter to disable this function.
Command Syntax
ospf abr-type cisco|ibm|shortcut|standard
(no) ospf abr-type cisco|ibm|shortcut
cisco Specifies an alternative ABR using Cisco implementation.
ibm Specifies an alternative ABR using IBM implementation.
shortcut Specifies a shortcut ABR.
standard Specifies a standard behavior ABR that conforms to RFC 2328 (Default).
Command Mode
Router mode
Usage
Specify the ABR type for better functioning between different implementations. This command is specially useful in a multivendor environment.
Examples
ospfd# configure terminal
ospfd(config)# router ospf 100
ospfd(config-router)# ospf abr-type standard
Related Commands

ospf authentication-key

Use the ospf authentication-key command to assign a password to be used by neighboring routers.
Use the no parameter to remove a previously assigned password.
Command Syntax
ospf authentication-key AUTHKEY
no ospf authentication-key
AUTHKEY Specifies the authentication password. Any continuous string of characters (not more than 8 bytes)
Default
Authentication password not specified.
Command Mode
Interface mode
Usage
The authentication-key command creates a key (password) which is inserted into the OSPF header, when ZebOS software originates routing protocols packets. You can assign a separate password to each network for different interfaces.
All neighboring routers on the same network must have the same password to enable exchange of OSPF information. The password can be used only if authentication has been enabled for an area. Use the area authentication command to enable authentication.
Simple password authentication allows a password to be configured per area. Configure the routers in the same routing domain with the same password.
Examples
ospf authentication-key mykeykey
ospf authentication-key
Related Commands
ip ospf authentication-key, area authentication

ospf cost

Use the ospf cost command to explicitly specify the cost of sending a packet on an interface.
Use the no form of this command to reset the cost of the path to default.

Command Syntax

ospf cost COST

no ospf cost

COST = <1-65535> Specifies the link-state metric.The default value is 10.

Command Mode

Interface mode

Usage

The interface cost indicates the overhead required to send packets across a certain interface. It is inversely proportional to the bandwidth of that interface. By default, the cost of an interface is calculated based on the bandwidth (108/ bandwidth); use this command to set cost manually.

Examples

ospfd# configure terminal

ospfd(config)# interface fxp0

ospfd(config-if)# ospf cost 10

Equivalent Commands

ip ospf cost

ospf dead-interval

Use the ospf dead-interval command to set the interval during which no hello packets are received and after which a neighbor is declared dead.

Use the no form of this command to disable this function

Command Syntax

ospf dead-interval INTERVAL

no ospf dead-interval

INTERVAL= <1-65535> Specifies the interval in seconds. The default interval is 40 seconds

Command Mode

Interface mode

Usage

The dead-interval is the amount of time that the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down. This value is advertised in the router's hello packets. It must be a multiple of hello-interval and be the same for all routers on a specific network.

Examples

ospfd# configure terminal

ospfd(config)# interface fxp0

ospfd(config-if)# ospf dead-interval 10 10.10.10.50

Equivalent Commands

ip ospf dead-interval

ospf hello-interval

Use the ospf hello-interval command to specify the interval between hello packets that the ZebOS software sends on the interface.

Use the no form of this command to return to the default setting.

Command Syntax

ospf hello-interval INTERVAL

no ospf hello-interval

INTERVAL= <1-65535> Specifies the interval in seconds. The default interval is 10 seconds.

Default

Command Mode

Interface mode

Usage

Hello-interval is advertised in the hello packets. Configure the same hello-interval for all routers on a specific network. A shorter hello interval ensures faster detection of topological changes but this also results in more routing traffic.

Examples

ospfd# configure terminal
ospfd(config)# interface fxp0
ospfd(config-if)# ospf hello-interval 3 10.10.10.50
Equivalent Commands
ip ospf hello-interval

ospf network

Use the ospf network command to configure the OSPF network type to a type other than the default for a given medium. Use the no form of this command to return to the default value.
Command Syntax
ospf network broadcast|non-broadcast|point-to-multipoint|point-to-point
no ospf network
broadcast Specifies OSPF braodcast as a multi-access network.
non-broadcast Sets the network type to NBMA.
point-to-multipoint Sets the network type to point-to-multipoint.
point-to-point Sets the network type to point-to-point.
Default
The default is the broadcast type.
Command Mode
Interface mode
Usage
Use ospf network command to configure broadcast networks as nonbroadcast multiaccess networks (NBMA) and vice versa. You would need to do this if you have routers in your network that do not support multicast addressing.
The ospf network command saves you from having to configure neighbors. Configuring NBMA networks requires a fully meshed network or a virtual circuit connecting every router. In case the network is not fully meshed, configure the OSPF network type as a point-to -multipoint network. Routing between two routers that are not directly connected will go through the router that has virtual circuits to both routers.
Examples
The following example shows setting the network to point-to-point type on the fxp0 interface.
ospfd# configure terminal
ospfd(config)# interface fxp0
ospfd(config-if)# ospf network point-to-point
Equivalent Commands
ip ospf network

ospf priority

Use the ospf priority command to set the router priority, which helps determine the designated router for this network. Use the no form of this command to return to the default value.
Command Syntax
ospf priority <1-255>
no ospf priority
Default
The default priority is 1.
Command Mode
Interface mode
Usage
Set the priority to help determine the OSPF Designated Router (DR) for a network. If two routers attempt to become the DR, the router with the higher router priority becomes the DR. If the router priority is the same for two routers, the router with the higher router ID becomes DR.
Only a router with a nonzero router priority value is eligible to become the designated or backup designated router.
Configure router priority for multiaccess networks only, and not for point-to-point networks.
Examples
The following example shows setting the OSPF priority value to 3 on the fxp0 interface for IP address 10.10.10.50.

ospfd# configure terminal
ospfd(config)# interface fxp0
ospfd(config-if)# ospf priority 3 10.10.10.50
Related Commands
show ip ospf
Equivalent Commands
ip ospf priority

ospf router-id

Use the ospf router-id command to specify a router ID for the OSPF process.
Use the no form of this command to disable this function.
Command Syntax
ospf router-id IPADDRESS
no ospf router-id
IPADDRESS Specifies the router ID in IPv4 address format.
Command Mode
Router mode
Usage
Configure each router with a unique router-id. In an OSPF router process which has active neighbors, a new router-id is used at the next reload or when you start the OSPF manually.
Examples
The following example shows a specified router ID 2.3.4.5.
ospfd# configure terminal
ospfd(config)# router ospf 100
ospfd(config-router)# ospf router-id 2.3.4.5
Related Commands
show ip ospf neighbor

ospf transmit-delay

Use the ospf transmit-delay command to set the estimated time it takes to transmit a link-state-update packet.
Use the no form of this command to disable this function
Command Syntax
ospf transmit-delay DELAY
no ospf transmit-delay
DELAY= <1-65535> the delay in seconds. The default transmit delay value is 1 second
Command Mode
Interface mode
Usage
The transmit delay value adds a specified time to the age field of an update. If the delay is not added, the time in which the LSA transmits over the link is not considered. This command is especially useful for low speed links. Add transmission and propagation delays when setting the transmit delay value.
Examples
The following example shows setting the OSPF transmit-delay time to 3 seconds on the fxp0 interface for the IP address 10.10.10.50.
ospfd# configure terminal
ospfd(config)# interface fxp0
ospfd(config-if)# ospf transmit-delay 3 10.10.10.50
Equivalent Commands
ip ospf transmit-delay

passive-interface

Use this command to suppress the routing updates on the specified interface.
Command Syntax

passive-interface INTERFACENAME (A.B.C.D)
INTERFACENAME = The name of the interface.
A.B.C.D = IP address of the interface.
Command Mode
Router mode
Usage
The passive-interface command is used to configure OSPF on simplex Ethernet interfaces. Since the simplex interfaces represent only one network segment between two devices, configure the transmitting interface as a passive interface. This ensures that OSPF does not send hello packets for the transmitting interface. Both the devices can see each other via the hello packet generated for the receiving interface.
Examples
ospfd(config)# router ospf 100
ospfd(config-router)# passive-interface fxp0
Related Commands

redistribute

Use the redistribute command to redistribute routes from other routing protocols, static routes and kernel routes into an ospf routing table.
Use the no form of this command to disable this function.
Command Syntax
redistribute PROTOCOL (METRICS|ROUTE)
no redistribute PROTOCOL
PROTOCOL= bgp|rip| ospf| connected|static|kernel
bgp Specifies BGP.
connected Specifies connected routes.
ospf6 Specifies OSPF v3. (Visible only if OSPFv3 is enabled on the system)
rip Specifies RIP.
ripng Specifies RIPng. (Visible only if ripng is enabled on the system)
static Specifies static routes.
kernel Specifies kernel routes.
METRICS= [METRIC METRIC-TYPE]|[METRIC-TYPE METRIC]
METRIC= metric <1-16777214> (ROUTE)
METRIC-TYPE= metric-type <1-2> (ROUTE)
ROUTE= route-map WORD
WORD= pointer to route-map entries list. A route-map is a series of rule-sets defined in privileged Exec mode.
Command Mode
Router mode
Usage
Examples
The following example shows redistribution of bgp routes into ospf routing table, with metric as 12.
ospfd# configure terminal
ospfd(config)# router ospf 100
ospfd(config-router)# redistribute bgp metric 12
Related Commands

refresh timer

Use the refresh timer command to adjust refresh parameters.
Use the no form of this command to disable this function.
Command Syntax
(no) refresh timer TIMERVALUE
TIMERVALUE = <10-1800> Timer value in seconds. The default refresh time is 10 seconds.
Command Mode

Router mode
Usage
Examples
ospfd# configure terminal
ospfd(config)# router ospf 100
ospfd(config-router)# refresh timer 12
Related Commands

router-id

Use the router-id command to set a fixed router-id.
Use the no form of this command to force OSPF to use the previous OSPF router-id behavior.
Command Syntax
router-id IPADDRESS
no router-id
IPADDRESS Specifies the router ID in IPv4 address format.
Default
Command Mode
Router mode
Usage
Examples
The following example shows a fixed router ID 10.10.10.60
ospfd# configure terminal
ospfd(config)# router ospf 100
ospfd(config-router)# router-id 10.10.10.60
Related Commands

router ospf

Use the router ospf command to enter router mode and to configure an OSPF routing process. Specify the process ID with this command to configure multiple instances.
Use the no form of this command to terminate an OSPF routing process. Use the no form of this command with the process ID parameter, to terminate and delete a specific OSPF routing process.
Command Syntax
(no) router ospf
(no) router ospf PROCESSID
PROCESSID = <1-65535> Any positive integer identifying a routing process. The process ID should be unique for each routing process.
Default
No routing process defined.
Command Mode
Configure mode
Usage
For releases starting with 1.1, router ospf command forces the router into compatibility mode. This mode supports only one OSPF instance and prevents the creation of other instances of OSPF. For multiple instances-- first, use the norouter ospf command to end the single instance routing process, and then, configure multiple instances by specifying the process ID parameter for each instance.
Examples
This example shows the use of router ospf command to enter router mode. Note the change in the prompt.
ospfd# configure terminal
ospfd(config)# router ospf
ospfd(config-router)#
Related Commands

set metric-type

Use the set metric-type command to set the metric type for the destination routing protocol.
Use the no form of this command to return to the default.

Command Syntax

(no) set metric-type 1|2

1 = Select to set external type 1 metric.

2 = Select to set external type 2 metric.

Default

Command Mode

Route-map mode

Usage

Examples

In this example the metric type of the destination protocol is set to OSPF external Type 1.

```
ospfd# configure terminal
ospfd(config)# route-map rmap1 permit 3
ospfd(config-route-map)# set metric-type 1
```

Related Commands

set next-hop

Use the set next-hop command to specify the next-hop address. Use the no parameter of this command to reset the default next-hop value.

Command Syntax

(no) set next-hop A.B.C.D

A.B.C.D = IP address of the next hop router.

Default

Command Mode

Route-map mode

Usage

Every routing table entry has a next-hop value. Once the next-hop value is calculated, the router gives the value to the forwarding engine.

To set the next-hop, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.

Examples

In the following example, routes that pass the access list have the next hop set to 10.10.12.50:

```
ospfd# configure terminal
ospfd(config)# route-map rmap1 permit 3
ospfd(config-route-map)# set next-hop 10.10.12.50
```

Related Commands

set tag

Use the set tag command to set specified tag value. Use the no form of this command to return to the default.

Command Syntax

(no) set tag TAGVALUE

TAGVALUE = <0-4294967295> Tag value for destination routing protocol.

Default

Command Mode

Route-map mode

Usage

Tag in this command is the route tag which is labeled by another routing protocol (BGP or other IGP when redistributing), because AS-external-LSA has route-tag field in its LSAs. And also with using route-map, ospfd can tag the LSAs with appropriate tag value. Sometimes tag matches with using route-map, and sometimes the value may be used by another application.

Examples

In the following example the tag value of the destination routing protocol is set to 6:

ospfd# configure terminal
ospfd(config)# route-map rmap1 permit 3
ospfd(config-route-map)# set tag 6

Related Commands

show debugging ospf

Use the show debugging ospf command to display the set OSPF debugging option.

Command Syntax

show debugging ospf

Command Mode

Priviledged Exec mode

Usage

This is a sample output from the show debugging ospf command. Some lines in this output wrap around, they might not wrap around in the actual display.

ospfd# show debugging ospf
OSPF debugging status:
OSPF packet Link State Update debugging is on
OSPF all events debugging is on

```
ospfd# te mo
ospfd# 2002/05/09 14:08:11 OSPF: RECV[LS-Upd]: From 10.10.10.70 via eth0:10.10.10.50(10.10.10.10 -> 224.0.0.5)
2002/05/09 14:08:11 OSPF: LSA[10.10.10.10:10.10.10.70]: instance(0x8139cd0) created withLink State Update
2002/05/09 14:08:11 OSPF: RECV[LS-Upd]: From 10.10.10.70 via eth0:10.10.10.50 (10.10.10.10-> 224.0.0.5)
2002/05/09 14:08:11 OSPF: LSA[10.10.10.70:10.10.10.70]: instance(0x813c688) created withLink State Update
2002/05/09 14:08:52 OSPF: RECV[LS-Upd]: From 10.10.10.70 via eth0:10.10.10.50 (10.10.10.10-> 224.0.0.5)
2002/05/09 14:08:52 OSPF: LSA[20.2.2.0:10.10.10.70]: instance(0x813a8e8) created with LinkState Update
2002/05/09 14:08:52 OSPF: LSA[40.2.2.0:10.10.10.70]: instance(0x8138be0) created with LinkState Update
2002/05/09 14:11:12 OSPF: RECV[LS-Upd]: From 10.10.10.70 via eth0:10.10.10.50 (10.10.10.10-> 224.0.0.5)
2002/05/09 14:11:12 OSPF: LSA[10.10.11.0:10.10.10.70]: instance(0x813c410) created withLink State Update
2002/05/09 14:12:33 OSPF: SEND[LS-Upd]: Begin send queue
2002/05/09 14:12:33 OSPF: SEND[LS-Upd]: # of LSAs 1, destination 224.0.0.5
2002/05/09 14:12:33 OSPF: SEND[LS-Upd]: End send queue
2002/05/09 14:12:33 OSPF: SEND[LS-Upd]: To 224.0.0.5 via eth0:10.10.10.50.
```

Examples

ospfd# show debugging ospf

Related Commands

show ip ospf

Use the show ip ospf command to display general information about all OSPF routing processes. Include the processID parameter with this command to display information about specified instances.

Command Syntax

show ip ospf
show ip ospf PROCESSID
PROCESSID = <0-65535> The ID of the router process for which information will be displayed. If this parameter is included, only the information for the specified routing process is displayed.

Command Mode

Priviledged Exec mode

Usage

The following are sample outputs from the show ip ospf command with and without the process ID parameter. Notice that the first output (without process ID), shows information about both instances and the second and third outputs show information only about the instances specified by the process ID.

```
ospfd# show ip ospf
 OSPF Routing Process 1, Router ID: 10.10.11.60
 Supports only single TOS (TOS0) routes
 This implementation conforms to RFC2328
 RFC1583Compatibility flag is disabled
 Opaque-LSA capability is on
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
 Number of external LSA 0
 Number of non-default external LSA 0
```

```
 External LSA database is unlimited.
 Number of areas attached to this router: 1
 Area ID: 0.0.0.1
   Shortcutting mode: Default, S-bit consensus: ok
   Number of interfaces in this area: Total: 1, Active: 1
   Number of fully adjacent neighbors in this area: 0
   Area has no authentication
   Number of full virtual adjacencies going through this area: 0
   SPF algorithm executed 1 times
   Number of LSA 1
 OSPF Routing Process 100, Router ID: 10.10.11.60
 Supports only single TOS (TOS0) routes
 This implementation conforms to RFC2328
 RFC1583Compatibility flag is disabled
 Opaque-LSA capability is on
 SPF schedule delay 0 secs, Hold time between two SPFs 0 secs
 Refresh timer 10 secs
 Number of external LSA 0
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of areas attached to this router: 1
 Area ID: 0.0.0.0 (Backbone)
   Number of interfaces in this area: Total: 0, Active: 0
   Number of fully adjacent neighbors in this area: 0
   Area has no authentication
   SPF algorithm executed 1 times
   Number of LSA 1
ospfd# show ip ospf 1
 OSPF Routing Process 1, Router ID: 10.10.11.60
 Supports only single TOS (TOS0) routes
 This implementation conforms to RFC2328
 RFC1583Compatibility flag is disabled
 Opaque-LSA capability is on
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
 Number of external LSA 0
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of areas attached to this router: 1
 Area ID: 0.0.0.1
   Shortcutting mode: Default, S-bit consensus: ok
   Number of interfaces in this area: Total: 1, Active: 1
   Number of fully adjacent neighbors in this area: 0
   Area has no authentication
   Number of full virtual adjacencies going through this area: 0
   SPF algorithm executed 1 times
   Number of LSA 1
ospfd# show ip ospf 100
 OSPF Routing Process 100, Router ID: 10.10.11.60
 Supports only single TOS (TOS0) routes
 This implementation conforms to RFC2328
 RFC1583Compatibility flag is disabled
 Opaque-LSA capability is on
 SPF schedule delay 0 secs, Hold time between two SPFs 0 secs
 Refresh timer 10 secs
 Number of external LSA 0
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of areas attached to this router: 1
 Area ID: 0.0.0.0 (Backbone)
   Number of interfaces in this area: Total: 0, Active: 0
   Number of fully adjacent neighbors in this area: 0
   Area has no authentication
   SPF algorithm executed 1 times
   Number of LSA 1
```

Examples

ospfd# show ip ospf

ospfd# show ip ospf 100

Related Commands

router ospf

show ip ospf border-routers

Use the show ip ospf border-routers command to display the ABRs and ASBRs for all OSPF instances. Include the process ID

parameter with this command to view data about specified instances.

Command Syntax

show ip ospf border-routers

show ip ospf PROCESSID border-routers

PROCESSID = <0-65535> The ID of the router process for which information will be displayed.

Command Mode

Priviledged Exec mode

Usage

This is a sample output from the show ip ospf border-routers command.

```
ospfd# show ip ospf border-routers
OSPF process 100
============= OSPF router routing table =============
R    10.10.10.70          [10] area: 0.0.0.0, ASBR
                       via 10.10.10.10, eth0
```

Examples

ospfd# show ip ospf border-routers

ospfd# show ip ospf 721 border-routers

Related Commands

show ip ospf database

Use this command to display a database summary for OSPF information. This command displays BGP tags for prefixes. Include the process ID parameter with this command to display information about specified instances.

Command Syntax

show ip ospf database(self-originate|max-age)

show ip ospf PROCESSID database (self-originate|max-age)

PROCESSID = <0-65535> The ID of the router process for which information will be displayed.

self-originate Displays self-originated link states.

max-age Displays LSAs in MaxAge list.

Command Mode

Priviledged Exec mode

Usage

The following are sample outputs from the show ip ospf database command with and without the process ID parameter. Notice that the first output (without process ID), shows database information about both the instances and the second and third outputs show database information only about the instances specified by the process ID. The last two displays show the use of the self-originate and max-age parameters.

```
ospfd# show ip ospf database
       OSPF Router process 1 with ID (10.10.11.60)
            Router Link States (Area 0.0.0.1)
Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.10.11.60     10.10.11.60      32 0x80000002 0x472b 1
      OSPF Router process 100 with ID (10.10.11.60)
            Router Link States (Area 0.0.0.0)
Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.10.11.60     10.10.11.60     219 0x80000001 0x4f5d 0
ospfd# show ip ospf 1 database
      OSPF Router process 1 with ID (10.10.11.60)
            Router Link States (Area 0.0.0.1)
Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.10.11.60     10.10.11.60      43 0x80000002 0x472b 1
ospfd# show ip ospf 100 database
      OSPF Router process 100 with ID (10.10.11.60)
            Router Link States (Area 0.0.0.0)
Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.10.11.60     10.10.11.60     244 0x80000001 0x4f5d 0
ospfd# show ip ospf database self-originate
      OSPF Router process 100 with ID (10.10.11.50)
            Router Link States (Area 0.0.0.1)
Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.10.11.50     10.10.11.50     20  0x80000007  0x65c3 2
            Area-Local Opaque-LSA (Area 0.0.0.1 )
```

```
Link ID         ADV Router      Age  Seq#       CkSum Opaque ID
67.1.4.217      10.10.11.50     37 0x80000001  0x2129 66777
            AS-Global Opaque-LSA
Link ID         ADV Router      Age  Seq#       CkSum Opaque ID
67.1.4.217      10.10.11.50     37 0x80000001  0x2daa 66777
ospfd# show ip ospf database max-age
      OSPF Router process 100 with ID (10.10.11.50)
            MaxAge Link States:
```

Examples

ospfd# show ip ospf database external 1.2.3.4 self-originate
ospfd# show ip ospf database self-originate
ospfd# show ip 1 ospf database max-age
ospfd# show ip 100 ospf database router adv-router 2.3.4.5

Related Commands

show ip ospf database asbr-summary

Use the show ip ospf database asbr-summary command to display information about the Autonomous System Boundary Router (ASBR) summary LSAs.

Command Syntax

show ip ospf database asbr-summary (A.B.C.D)(self-originate|ADVROUTER)
ADVROUTER = adv-router A.B.C.D
adv-router Displays all the LSAs of the specified router.
A.B.C.D A link state ID (as an IP address).
self-originate Displays self-originated link states.

Command Mode

Priviledged Exec mode

Usage

Examples

ospfd# show ip ospf database external 1.2.3.4 self-originate
ospfd# show ip ospf database self-originate
ospfd# show ip ospf database max-age
ospfd# show ip ospf database router 1.2.3.4 adv-router 2.3.4.5

Related Commands

show ip ospf database external

Use this command to display information about the external LSAs.

Command Syntax

show ip ospf database external (A.B.C.D)(self-originate|ADVROUTER)
ADVROUTER = adv-router A.B.C.D
adv-router Displays all the LSAs of the specified router.
A.B.C.D A link state ID (as an IP address).
self-originate Displays self-originated link states.

Command Mode

Priviledged Exec mode

Usage

This is a sample output from the show ip ospf database external command with the self-originate option selected.

```
ospfd# show ip ospf database external self-originate
      OSPF Router process 100 with ID (10.10.11.50)
            AS External Link States
  LS age: 298
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
  Link State ID: 10.10.100.0 (External Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x7033
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
```

TOS: 0
Metric: 20
Forward Address: 10.10.11.50
External Route Tag: 0

Examples

ospfd# show ip ospf database external 1.2.3.4 self-originate
ospfd# show ip ospf database self-originate
ospfd# show ip ospf database max-age
ospfd# show ip ospf database router 1.2.3.4 adv-router 2.3.4.5

Related Commands

show ip ospf database network

Use the show ip ospf database network command to display information about the network LSAs.

Command Syntax

show ip ospf database network (A.B.C.D)(self-originate|ADVROUTER)
ADVROUTER = adv-router A.B.C.D
adv-router Displays all the LSAs of the specified router.
A.B.C.D A link state ID (as an IP address).
self-originate Displays self-originated link states.

Command Mode

Priviledged Exec mode

Usage

The following is a sample output from the show ip ospf database network command, with and without the advrouter option selected:

```
ospfd# show ip ospf database network
       OSPF Router process 200 with ID (192.30.30.2)
                Net Link States (Area 0.0.0.0)
  LS age: 1175
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: network-LSA
  Link State ID: 192.10.10.9 (address of Designated Router)
  Advertising Router: 192.30.30.3
  LS Seq Number: 80000002
  Checksum: 0xdfb1
  Length: 32
  Network Mask: /24
        Attached Router: 192.20.20.1
        Attached Router: 192.30.30.3
  LS age: 1327
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: network-LSA
  Link State ID: 192.20.20.2 (address of Designated Router)
  Advertising Router: 192.20.20.2
  LS Seq Number: 8000000d
  Checksum: 0xbce6
  Length: 32
  Network Mask: /24
        Attached Router: 192.20.20.1
        Attached Router: 192.20.20.2
  LS age: 1278
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: network-LSA
  Link State ID: 192.30.30.3 (address of Designated Router)
  Advertising Router: 192.30.30.3
  Advertising Router: 192.30.30.3
  LS Seq Number: 80000001
  Checksum: 0x0556
  Length: 32
  Network Mask: /24
        Attached Router: 192.30.30.2
        Attached Router: 192.30.30.3
  LS age: 1436
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: network-LSA
  Link State ID: 192.40.40.2 (address of Designated Router)
  Advertising Router: 192.20.20.2
```

```
  LS Seq Number: 8000000e
  Checksum: 0xf173
  Length: 32
  Network Mask: /24
        Attached Router: 192.20.20.2
        Attached Router: 192.30.30.2
ospfd# show ip ospf database network adv-router 192.30.30.3
       OSPF Router process 200 with ID (192.30.30.2)
              Net Link States (Area 0.0.0.0)
  LS age: 1387
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: network-LSA
  Link State ID: 192.10.10.9 (address of Designated Router)
  Advertising Router: 192.30.30.3
  LS Seq Number: 80000001
  Checksum: 0xe1b0
  Length: 32
  Network Mask: /24
        Attached Router: 192.20.20.1
        Attached Router: 192.30.30.3
  LS age: 1648
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: network-LSA
 Link State ID: 192.30.30.3 (address of Designated Router)
  Advertising Router: 192.30.30.3
  LS Seq Number: 8000000f
  Checksum: 0xe864
  Length: 32
  Network Mask: /24
        Attached Router: 192.30.30.2
        Attached Router: 192.30.30.3
```

Examples

ospfd# show ip ospf database external 1.2.3.4 self-originate

ospfd# show ip ospf database self-originate

ospfd# show ip ospf database max-age

ospfd# show ip ospf database router 1.2.3.4 adv-router 2.3.4.5

Related Commands

show ip ospf database opaque-area

Use the show ip ospf database opaque-area command to display information about the area-local (link state type 10) scope LSAs. Type-10 Opaque LSAs are not flooded beyond the borders of their associated area.

Command Syntax

show ip ospf database opaque-area (A.B.C.D)(self-originate|ADVROUTER)

ADVROUTER = adv-router A.B.C.D

adv-router Displays all the LSAs of the specified router.

A.B.C.D A link state ID (as an IP address).

self-originate Displays self-originated link states.

Command Mode

Priviledged Exec mode

Usage

The following is a sample output from the show ip ospf database opaque-area command, with the selforiginate option selected.

```
ospfd# show ip ospf database opaque-area self-originate
       OSPF Router process 100 with ID (10.10.11.50)
              Area-Local Opaque-LSA (Area 0.0.0.0)
  LS age: 262
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: Area-Local Opaque-LSA
  Link State ID: 10.0.25.176 (Area-Local Opaque-Type/ID)
  Opaque Type: 10
  Opaque ID: 6576
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0xb413
  Length: 26
```

Examples

ospfd# show ip ospf database external 1.2.3.4 self-originate

ospfd# show ip ospf database self-originate
ospfd# show ip ospf database max-age
ospfd# show ip ospf database router 1.2.3.4 adv-router 2.3.4.5

Related Commands

show ip ospf database opaque-link

Use the show ip ospf database opaque-link command to display information about the link-state type 9 LSAs. This type denotes a link-local scope. The LSAs are not flooded beyond the local network.

Command Syntax

show ip ospf database opaque-link (A.B.C.D)(self-originate|ADVROUTER)
ADVROUTER = adv-router A.B.C.D
adv-router Displays all the LSAs of the specified router.
A.B.C.D A link state ID (as an IP address).
self-originate Displays self-originated link states.

Command Mode

Priviledged Exec mode

Usage

The following is a sample output from the show ip ospf database opaque-link command, with a link-state selected.

```
ospfd# show ip ospf database opaque-link 10.0.220.247
      OSPF Router process 100 with ID (10.10.11.50)
            Link-Local Opaque-LSA (Link hme0:10.10.10.50)
  LS age: 276
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: Link-Local Opaque-LSA
  Link State ID: 10.0.220.247 (Link-Local Opaque-Type/ID)
  Opaque Type: 10
  Opaque ID: 56567
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x744e
  Length: 26
            Link-Local Opaque-LSA (Link hme1:10.10.11.50)
```

Examples

ospfd# show ip ospf database external 1.2.3.4 self-originate
ospfd# show ip ospf database self-originate
ospfd# show ip ospf database max-age
ospfd# show ip ospf database router 1.2.3.4 adv-router 2.3.4.5

Related Commands

show ip ospf database router

Use the show ip ospf database router command to display information only about the router LSAs.

Command Syntax

show ip ospf database router (A.B.C.D)(self-originate|ADVROUTER)
ADVROUTER = adv-router A.B.C.D
adv-router Displays all the LSAs of the specified router.
A.B.C.D A link state ID (as an IP address).
self-originate Displays self-originated link states.

Command Mode

Priviledged Exec mode

Usage

The following is a sample output from the show ip ospf database router command, with the ip address selected.

```
ospfd# show ip ospf database router 10.10.11.50
      OSPF Router process 100 with ID (10.10.11.50)
            Router Link States (Area 0.0.0.0)
  LS age: 878
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x3 : ABR ASBR
  LS Type: router-LSA
```

```
Link State ID: 10.10.11.50
Advertising Router: 10.10.11.50
LS Seq Number: 80000004
Checksum: 0xe39e
Length: 36
 Number of Links: 1
  Link connected to: Stub Network
   (Link ID) Network/subnet number: 10.10.10.0
   (Link Data) Network Mask: 255.255.255.0
    Number of TOS metrics: 0
     TOS 0 Metric: 10

            Router Link States (Area 0.0.0.1)
LS age: 877
Options: 0x2 (*|-|-|-|-|-|E|-)
Flags: 0x3 : ABR ASBR
LS Type: router-LSA
Link State ID: 10.10.11.50
Advertising Router: 10.10.11.50
LS Seq Number: 80000003
Checksum: 0xee93
Length: 36
 Number of Links: 1
  Link connected to: Stub Network
   (Link ID) Network/subnet number: 10.10.11.0
   (Link Data) Network Mask: 255.255.255.0
    Number of TOS metrics: 0
     TOS 0 Metric: 10
```

Examples

ospfd# show ip ospf database external 1.2.3.4 self-originate

ospfd# show ip ospf database self-originate

ospfd# show ip ospf database max-age

ospfd# show ip ospf database router 1.2.3.4 adv-router 2.3.4.5

Related Commands

show ip ospf database summary

Use the show ip ospf database summary command to display information about the summary LSAs.

Command Syntax

show ip ospf database summary (A.B.C.D)(self-originate|ADVROUTER)

ADVROUTER = adv-router A.B.C.D

adv-router Displays all the LSAs of the specified router.

A.B.C.D A link state ID (as an IP address).

self-originate Displays self-originated link states.

Command Mode

Priviledged Exec mode

Usage

The following are the sample outputs from the show ip ospf database summary command, using the selforiginate, adv-router and ip address options.

```
ospfd# show ip ospf database summary 10.10.10.0
      OSPF Router process 100 with ID (10.10.11.50)
            Summary Link States (Area 0.0.0.0)
            Summary Link States (Area 0.0.0.1)
  LS age: 1124
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: summary-LSA
  Link State ID: 10.10.10.0 (summary Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x41a2
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 10
ospfd# show ip ospf database summary self-originate
      OSPF Router process 100 with ID (10.10.11.50)
            Summary Link States (Area 0.0.0.0)
  LS age: 1061
  Options: 0x2 (*|-|-|-|-|-|E|-)
```

```
  LS Type: summary-LSA
  Link State ID: 10.10.11.0 (summary Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x36ac
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 10
              Summary Link States (Area 0.0.0.1)
  LS age: 1061
  Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: summary-LSA
  Link State ID: 10.10.11.0 (summary Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x36ac
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 10
              Summary Link States (Area 0.0.0.1)
  LS age: 1061
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: summary-LSA
  Link State ID: 10.10.10.0 (summary Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x41a2
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 10
ospfd# show ip ospf database summary adv-router 10.10.11.50
      OSPF Router process 100 with ID (10.10.11.50)
              Summary Link States (Area 0.0.0.0)
  LS age: 989
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: summary-LSA
  Link State ID: 10.10.11.0 (summary Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x36ac
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 10
              Summary Link States (Area 0.0.0.1)
  LS age: 989
  Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: summary-LSA
  Link State ID: 10.10.11.0 (summary Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x36ac
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 10
```

Examples

ospfd# show ip ospf database external 1.2.3.4 self-originate

ospfd# show ip ospf database self-originate

ospfd# show ip ospf database max-age

ospfd# show ip ospf database router 1.2.3.4 adv-router 2.3.4.5

Related Commands

show ip ospf interface

Use the show ip ospf interface command to display interface information for OSPF.

Command Syntax

show ip ospf interface IFNAME

IFNAME= An alphanumeric string that is the interface name.

Command Mode

Priviledged Exec mode

Usage

The following is a sample output from the show ip ospf interface command.

```
ospfd# show ip ospf interface hme0
hme0 is up, line protocol is up
  Internet Address 10.10.10.50/24, Area 0.0.0.0
    Router ID 10.10.11.50, Network Type BROADCAST, Cost: 10
    Transmit Delay is 5 sec, State Waiting, Priority 1
    No designated router on this network
    No backup designated router on this network
    Timer intervals configured, Hello 35, Dead 35, Wait 35, Retransmit 5
      Hello due in 00:00:16
    Neighbor Count is 0, Adjacent neighbor count is 0
```

Examples

```
ospfd# show ip ospf interface myifname
```

Related Commands

show ip ospf neighbor

Use the show ip ospf neighbor command to display information on OSPF neighbors. Include the process ID parameter with this command to display information about specified instances.

Command Syntax

```
show ip ospf neighbor A.B.C.D|all|DETAIL|INTERFACE
show ip ospf PROCESSID neighbor A.B.C.D|all|DETAIL|INTERFACE
```

PROCESSID = <0-65535> The ID of the router process for which information will be displayed.
A.B.C.D = A.B.C.D (detail) Neighbor ID.
all = Include downstatus neighbor
DETAIL = detail (all) Detail of all neighbors
INTERFACE = Interface (A.B.C.D)
A.B.C.D = Address of the interface

Command Mode

Priviledged Exec mode

Usage

The following are sample outputs from the show ip ospf neighbor command with and without the process IDparameter. Notice that the first output (without process ID), shows database information about both the instances and the second and third outputs show database information only about the instances specified by the process ID. The last two displays show the use of the detail and all parameters.

```
ospfd# show ip ospf neighbor
OSPF process 1:
Neighbor ID     Pri   State     Dead Time   Address     Interface          RXmtL
RqstL DBsmL
10.10.11.50       5   Full/DR         00:00:40    10.10.10.50     eth1:10.10.10.90     0
0     0
OSPF process 100:
Neighbor ID     Pri   State           Dead Time   Address         Interface          RXmtL
RqstL DBsmL
10.10.11.50       5   Full/DR         00:00:40    10.10.10.50     eth2:10.10.11.90     0
0     0
ospfd# show ip ospf 1 neighbor
OSPF process 1:
Neighbor ID     Pri   State           Dead Time   Address         Interface          RXmtL
RqstL DBsmL
10.10.11.50       5   Full/DR         00:00:40    10.10.10.50     eth1:10.10.10.90     0
0     0
ospfd# show ip ospf 100 neighbor
OSPF process 100:
Neighbor ID     Pri   State           Dead Time   Address         Interface          RXmtL
RqstL DBsmL
10.10.11.50       5   Full/DR         00:00:40    10.10.10.50     eth2:10.10.11.90     0
0     0
ospfd# show ip ospf neighbor all
OSPF process 100:
Neighbor ID  Pri   State    Dead Time   Address      Interface          RXmtL RqstL DBsmL
10.10.11.51    1   Full/DR  00:00:38    10.10.10.10  hme0:10.10.10.50   0     0     0
```

```
10.10.11.51    1   Full/DR  00:00:38    10.10.11.10  hme1:10.10.11.50   0     0     0
ospfd#
ospfd# show ip ospf neighbor detail
 Neighbor 10.10.11.51, interface address 10.10.10.10
    In the area 0.0.0.0 via interface hme0
    Neighbor priority is 1, State is Full, 6 state changes
    DR is 10.10.10.10, BDR is 10.10.10.50
    Options 66 *|O|-|-|-|E|-
    Dead timer due in 00:00:32
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    Thread Inactivity Timer on
    Thread Database Description Retransmision off
    Thread Link State Request Retransmission off
    Thread Link State Update Retransmission on
 Neighbor 10.10.11.51, interface address 10.10.11.10
    In the area 0.0.0.0 via interface hme1
    Neighbor priority is 1, State is Full, 6 state changes
    DR is 10.10.11.10, BDR is 10.10.11.50
    Options 66 *|O|-|-|-|E|-
    Dead timer due in 00:00:32
    Database Summary List 0
    Link State Request List 0
Link State Retransmission List 0
    Thread Inactivity Timer on
    Thread Database Description Retransmision off
    Thread Link State Request Retransmission off
    Thread Link State Update Retransmission on
 Neighbor 10.10.11.51, interface address 10.10.11.10
    In the area 0.0.0.0 via interface hme1
    Neighbor priority is 1, State is Full, 6 state changes
    DR is 10.10.11.10, BDR is 10.10.11.50
    Options 66 *|O|-|-|-|E|-
    Dead timer due in 00:00:32
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    Thread Inactivity Timer on
    Thread Database Description Retransmision off
    Thread Link State Request Retransmission off
    Thread Link State Update Retransmission on
```

Examples

ospfd# show ip ospf neighbor detail

ospfd# show ip ospf neighbor 1.2.3.4

ospfd# show ip ospf neighbor myifname detail all

Related Commands

show ip ospf route

Use the show ip ospf route command to display the OSPF routing table. Include the process ID parameter with this command to display the OSPF routing table for specified instances.

Command Syntax

show ip ospf route

show ip ospf PROCESSID route

PROCESSID = <0-65535> The ID of the router process for which information will be displayed. If this parameter is included, only the information for this specified routing process is displayed.

Command Mode

Priviledged Exec mode

Usage

The following are sample outputs from the show ip ospf route command with and without the process ID parameter. Notice that the first output (without process ID), shows information about both the instances and the second and third outputs show information only about the instances specified by the process ID.

```
ospfd# show ip ospf route
OSPF process 100:
============ OSPF network routing table =============
N    10.10.10.0/24          [10] area: 0.0.0.0
                            directly attached to eth1
```

```
============ OSPF router routing table =============
============ OSPF external routing table ===========
OSPF process 110:
============ OSPF network routing table ============
N    10.10.11.0/24          [10] area: 0.0.0.1
                            directly attached to eth2
============ OSPF router routing table =============
============ OSPF external routing table ===========
ospfd#
ospfd# show ip ospf 100 route
OSPF process 100:
============ OSPF network routing table ============
N    10.10.10.0/24          [10] area: 0.0.0.0
                            directly attached to eth1
============ OSPF router routing table =============
============ OSPF external routing table ===========
ospfd#
ospfd# show ip ospf 110 route
OSPF process 110:
============ OSPF network routing table ============
N    10.10.11.0/24          [10] area: 0.0.0.1
                            directly attached to eth2
============ OSPF router routing table =============
============ OSPF external routing table ===========
ospfd#
```

Examples

ospfd# show ip ospf route

Related Commands

show ip protocols

Use the show ip protocols command to display OSPF process parameters and statistics.

Command Syntax

show ip protocols

There are no arguments or keywords for this command.

Command Mode

Priviledged Exec mode

Usage

This is an example of the output from the show ip protocols command:

```
ospfd# show ip protocols
Routing Protocol is "ospf 200"
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is
    Redistributed kernel filterd by filter1
  Incoming update filter list for all interfaces is
  Redistributing: kernel
  Routing for Networks:
    192.30.30.0/24
    192.40.40.0/24
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)
    Address         Mask            Distance List
```

Examples

ospfd# show ip protocols

show memory all

Use the show memory all command to display all memory statistics.

Command Syntax

show memory all

Command Mode

Priviledged Exec mode and Exec mode

Usage

Following is a sample output of the show memory all command showing information about all the routing protocols. Please note that this is not the complete output but a sample of the output.

```
ospfd# show memory all
Memory type                 : Alloc count    Alloc memory
============================================================
Hash                        :         1              20
Hash Index                  :         1              64
Hash Bucket                 :         0               0
Thread master               :         1             196
Thread                      :        28            1008
Link List                   :       394            7880
Link Node                   :       382            4584
Buffer                      :         2              56
Route node                  :         0               0
VR data block               :         0               0
Config password             :         1               6
Config handle               :         1              16
Temporary memory            :         1              32
Access List                 :         0               0
Label pool server           :         0               0
Label pool server           :         0               0
------------------------------------------------------
ZebOS RIB                   :         0               0
ZebOS IPv4 Static           :         0               0
ZebOS IPv6 Static           :         0               0
ZebOS RA                    :         0               0
ZebOS RA conf               :         0               0
ZebOS RA Prefix             :         0               0
ZebOS Home Agent            :         0               0
------------------------------------------------------
RIP structure               :         0               0
RIP route info              :         0               0
RIP interface               :         0               0
RIP i/f name                :         0               0
RIP passive i/f             :         0               0
------------------------------------------------------
RIPng structure             :         0               0
RIPng route info            :         0               0
RIPng aggregate info        :         0               0
RIPng interface             :         0               0
RIPng i/f name              :         0               0
------------------------------------------------------
OSPF table                  :        47             780
OSPF node                   :        26             764
OSPF prefix                 :        26             247
------------------------------------------------------
OSPF structure              :         1            1600
OSPF area                   :         1             108
OSPF interface              :         2             368
OSPF neighbor               :         0               0
OSPF SPF vertex             :         0               0
OSPF SPF nexthop            :         0               0
OSPF route                  :         2              88
OSPF path                   :         2              24
OSPF LSA                    :         1              52
OSPF LSA data               :         1              48
OSPF LSDB                   :         4             576
OSPF distance               :         0               0
------------------------------------------------------
OSPF network                :         2              22
OSPF virtual-link           :         0               0
OSPF if params              :         0               0
OSPF passive if             :         0               0
------------------------------------------------------
BGP peer                    :         0               0
------------------------------------------------------
BGP adjacency               :         0               0
BGP advertise               :         0               0
BGP advertise attr          :         0               0
BGP adjin                   :         0               0
------------------------------------------------------
BGP attribute               :         0               0
```

```
BGP aspath                  :          0             0
BGP aspath seg              :          0             0
BGP aspath str              :          0             0
Community                   :          0             0
-------------------------------------------------
LDP structure               :          0             0
LDP interface               :          0             0
LDP Adjacencies             :          0             0
LDP Sessions                :          0             0
LDP FECs                    :          0             0
-------------------------------------------------
RSVP structure              :          0             0
RSVP interface              :          0             0
RSVP write queue node       :          0             0
RSVP route record object    :          0             0
-------------------------------------------------
ISIS node                   :          0             0
ISIS table                  :          0             0
vprefix                     :          0             0
ISIS instance               :          0             0
ISIS neighbor               :          0             0
```

Examples

ospfd# show memory all

Related Commands

show memory lib, show memory ospf

show memory lib

Use the show memory lib command to display memory statistics for the ZebOS library.

Command Syntax

show memory lib

Command Mode

Priviledged Exec mode and Exec mode

Usage

The following is a sample output from the show memory lib command displaying ZebOS library statistics.

```
ospfd# show memory lib
Memory type                 : Alloc count    Alloc memory
============================================================
Hash                        :          1             20
Hash Index                  :          1             64
Hash Bucket                 :          0              0
Thread master               :          1            196
Thread                      :         28           1008
Link List                   :        394           7880
Link Node                   :        382           4584
Buffer                      :          2             56
Buffer backet               :          8            192
Buffer data                 :          8           1724
Buffer iov                  :          0              0
Prefix                      :        156           3120
Prefix IPv4                 :          0              0
Prefix IPv6                 :          0              0
Route table                 :          0              0
Route node                  :          0              0
VR data block               :          0              0
User data                   :          0              0
RMM data block              :          0              0
RMM Message                 :          0              0
RMM dummy client            :          0              0
Smux subtree                :          0              0
Command strvec              :       6761         117184
Command desc                :       3396          27168
Config memory               :          3             58
Config login                :          0              0
Config password             :          1              6
Config handle               :          1             16
Temporary memory            :          1             32
Access List                 :          0              0
Access List Str             :          0              0
Access Filter               :          0              0
Prefix List                 :          0              0
```

```
Prefix List Str              :          0              0
Prefix List Entry            :          0              0
Route map                    :          0              0
Route map name               :          0              0
Route map index              :          0              0
Route map rule               :          0              0
Route map rule str           :          0              0
Stream                       :          2             48
Key                          :          0              0
Key chain                    :          0              0
VTY                          :          2         239896
VTY Path                     :          0              0
Label block node             :          0              0
Label pool server            :          0              0
Label pool server            :          0              0
```

Examples

ospfd# show memory lib

Related Commands

show memory all, show memory ospf

show memory ospf

Use the show memory ospf command to display memory statistics for the OSPF protocol.

Command Syntax

show memory ospf

Command Mode

Priviledged Exec mode and Exec mode

Usage

The following is a sample output from the show memory ospf command displaying OSPF statistics

```
ospfd# show memory ospf
Memory type                  : Alloc count    Alloc memory
============================================================
OSPF table                   :         102            1660
OSPF node                    :          53            1528
OSPF prefix                  :          53             515
------------------------------------------------------------
OSPF structure               :           1            1600
OSPF area                    :           2             216
OSPF interface               :           2             368
OSPF neighbor                :           2             336
OSPF SPF vertex              :           0               0
OSPF SPF nexthop             :           0               0
OSPF route                   :           3             132
OSPF path                    :           3              36
OSPF LSA                     :           7             364
OSPF LSA data                :           7             224
OSPF LSDB                    :           9            1296
OSPF LS Request              :           0               0
OSPF packet                  :           1              16
OSPF FIFO queue              :           2              24
OSPF extern info             :           1              32
OSPF distance                :           0               0
------------------------------------------------------------
OSPF network                 :           2              22
OSPF virtual-link            :           0               0
OSPF if params               :           0               0
OSPF passive if              :           0               0
OSPF auth key                :           0               0
OSPF crypt key               :           0               0
OSPF area range              :           0               0
OSPF summary addr            :           0               0
OSPF static nbr              :           0               0
------------------------------------------------------------
OSPF opaque data             :           0               0
OSPF Opq-LSA show            :           0               0
OSPF notifier                :           0               0
OSPF description             :           0               0
OSPF API data                :           0               0
OSPF message                 :           0               0
OSPF tmp mem                 :           2              16
```

Examples

ospfd# show memory ospf

Related Commands

show memory all, show memory lib

summary-address

Use the summary-address command to summarize or suppress external routes with the specified address range.

Command Syntax

summary-address A.B.C.D/M (not-advertise)(tag <0-4294967295>)

A.B.C.D/M = The range of addresses given as IPv4 starting address and a mask indicating the range.

not-advertise Suppresses external routes.

tag <0-4294967295> The default tag value is 0.

Command Mode

Router mode

Usage

An address range is a pairing of an address and a mask that is almost the same as IP network number. For example, if the specified address range is 192.168.0.0/255.255.240.0, it matches: 192.168.1.0/24, 192.168.4.0/22, 192.168.8.128/25 and so on.

Redistributing routes from other protocols into OSPF requires the router to advertise each route individually in an external LSA. Use summary address command to advertise one summary route for all redistributed routes covered by a specified network address and mask. This helps decrease the size of the OSPF link state database.

Examples

The following example uses the summary-address command to aggregate external LSAs that match the network 172.16.0.0/24 and assign a Tag value of 3.

ospfd# configure terminal

ospfd(config)# router ospf 100

ospfd(config-router)# summary-address 172.16.0.0/16 tag 3

Related Commands

timers spf

Use the timers spf command to adjust route-calculation timers.

Use the no parameter of this command to return to the default timer values.

Command Syntax

timers spf SPF-DELAY spf-holdtime

no timers spf SPF-DELAY SPF-HOLDTIME

SPF-DELAY= <0-4294967295> Specifies the delay between receiving a change to SPF calculation.The default spf-delay value is 5 seconds

SPF-HOLDTIME= <0-4294967295> Specifies hold time between consecutive SPF calculations. The default spf-holdtime value is 10 seconds.

Command Mode

Router mode

Usage

The timer spf command configures the delay time between the receipt of a topology change and the calculation of the Shortest Path First (SPF). This command also configure the hold time between two consecutive SPF calculations.

Examples

timers spf 67295 7295

Related Commands

Index