Intel® Express Router

8210, 8220, 9530, and 9535

User Guide

Intel® Express Router 8210, 8220, 9530, and 9535

User Guide

731460-002

Copyright © 2000, Intel Corporation. All rights reserved.

Intel Corporation, 5200 NE Elam Young Parkway, Hillsboro, OR 97124-6497

Intel Corporation assumes no responsibility for errors or omissions in this manual. Nor does Intel make any commitment to update the information contained herein.

§ Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owners' benefit, without intent to infringe.

Second edition June 2000 **731460-002**

Preface xi

Statutory Notices & Warnings xi
FCC Statements xii
Industry Canada Notice xiii
EEC Declarations xiv
Approvals xvii
Wichtige Hinweise und Vorsichtsmaßnahmen xviii
Notes Statutaires et Avertissements xix

Chapter 1

Introduction to the Intel® Express Router 1

Hardware Overview 1
LED Descriptions 5
Features of the Intel Express Router 8
Management 8
CSU/DSU T1 Services 11
Frame Relay Services 11
X.25 Services 13
PPP Leased Line Multilinks 14
PPP Dial-up Modem Connections 14
Point-to-Point Protocol (PPP) 15
Internet Tunnels 16
Network and Bridging Services 17
Dynamic Host Control Protocol (DHCP) Server 20
Router Factory Default Setup 21

Chapter 2

Installation 23

Warnings 23
Product Parts 23
Installation Procedure 25
Preparation 25
Connecting the Intel Express Router 26
Connecting to the Local Area Network (Ethernet) 26
Connecting the WAN Port 27
Connecting the CSU/DSU Port to a T1 Service 29
Connecting a Dial-up Modem to the Console Port 29

Connecting the Console Port to a VT100-compatible Terminal or PC 30
Power Up the Router 31
Software Installation 32
Installing Intel, Device View 32
Installing Adobe Acrobat Reader§ for Use with On-line Manuals 34
Installing Internet Explorer 35
Installing Shiva§ Configurator 35

Chapter 3

Managing the Router Using Intel Device View 37

Getting Started 38
On-line Help 40
Intel Device View Display 41
Device View 42
Device Tree 43
Using Device Tree 45
Diagnostics Window 47
Using Diagnostics 49
Trap Window 50
Using Trap Window Options 51
System Window 51
Using the System Window Functions 53
Explorer View 54
Configuring the Router Using Intel Device View 57
Configuring Ports and Connections Using Connection Setup 58
Accessing Connection Setup 59
Configuring a WAN Port (WAN, CSU/DSU, HDSL2, and Console port) 60
Adding and Editing Remote Connections 61
Configuring LAN Ports 62
Exiting Connection Setup 63
Configuring the DHCP Server 63
Configuring IP Network Address Translations 65
Configuring IP Static Routes 67
Configuring IP Filters and Firewalls 68
Configuration Management 70
Upgrading and Managing the Router Firmware and Plug-ins 73
Managing Licensed Software 75
Monitoring the Router 76
Plotting Management Information 78

Setting Monitor Preferences 79
Setting the Polling Parameters 79

Chapter 4

Introduction to Local Management 81

Local Management Access Using Telnet 82
Local Management Access From the Console Port 84
Direct Connection to the Console port 85
Dial-in Modem Connection to the Console Port 86
Local Management Login 88

Chapter 5

Introduction to Advanced Setup 91

Advanced Setup Overview 91
Accessing Advanced Setup 92
On-line Help 96
General Configuration 96
Exiting Advanced Setup 96

Chapter 6

Configuring WAN Services and Links 99

CSU/DSU and HDSL2 ports 99
T1 Overview 99
Configuring a CSU/DSU Port 100
Configuring for PPP Leased Lines 103
Configuring a PPP Leased Line Multilink 106
Configuring Frame Relay Services 109
Automatic Configuration of Frame Relay Service 111
Manual Configuration of Frame Relay Services and Links 113
Configuring X.25 Services 118
Configuring PPP Dial-up Modem Links on the Console Port 123
Overview 123
Configuring the Console Port for the Modem and the PPP Dial-up Links 124
Modem Profiles 128
Configuring an Internet Tunnel 131
Internet Tunnel Example 135

Example of Configuring a Tunnel for Basic Internet Access 135
Basic Filter Requirements for the Example 139
Example Use of Internet Tunnels to Offer Data Security over X.25 links 143
Configuring Password Protection using CHAP or PAP 144
Configuring Advanced Link Features and Parameters 146
Setting Up Timer Profiles 150

Chapter 7

Configuring IP Routing 153

Introduction to IP Routing in the Express Router 153
IP Multicast Routing 155
Configuring IP Routing on LAN and WAN Links 156
Configuring IP Multicast Tunnels 162
Configuring Bandwidth Reservation using RSVP 164
IP Filters and Firewall Protection 167
Features of Stateful Filters 171
Port-to-application Mapping 171
SYN Flood Protection 172
To Configure Firewall Protection and IP Filters and on LAN and WAN Links 174
Static IP Filter Examples 180
Filtering Telnet 180
Stateful Filter Examples 183
Protecting Your Private Network From the Internet With a Single LAN Port 183
Setting Up a DMZ Firewall Using Two LAN Ports 187
Network Address Translation (NAT) 192
Setting Up Network Address Translations on the LAN and WAN Links 196
Examples of Use 198
Configuring IP Static Routes 200
Domain Name System (DNS) 202

Chapter 8

Configuring Novell IPX Routing 203

Introduction to Novell IPX Routing in the Express Router 203
IPX Watchdog Packets over X.25 SVCs 204
SPX Keep-alive Packets over X.25 SVCs 205
Configuring IPX Routing on the LAN and WAN Links 207
RIP and SAP Filters 210

Configuring RIP and SAP Filtering on the LAN and WAN Links 211
IPX Data Filters 215
Configuring IPX Data Filtering on the LAN and WAN Links 216
IPX Filters Example 219
Configuring IPX Static Routes and Services 220
To configure Static Routes and Services 221
Static Routes and Services Example 223

Chapter 9

Configuring Bridging Services 225

Introduction to Bridging in the Express Router 225
Bridge Spoofing 226
Configuring Bridging Services on the LAN and WAN Links 227
Configuring Static Destinations, Sources and Packet Types 229
Static Forwarding Table Example 231
Controlled Bridging 233
Restricting Multicasts to Remote Networks 235
Configuring Static Tables and Controlled Bridging 236

Chapter 10

Configuring the DHCP Server 241

Overview 241
Configuring the DHCP Server 242

Chapter 11

Management Access and Services 247

Configuring Management Access Rights 247
Configuring SNMP/TFTP and Telnet Access Rights 248
Configuring Local Management Passwords and Access 250
Setting the Console Port for Terminal Use - Console Mode 252
Configuring SNMP Traps 252
Configuring the Log System 253
Overview 253
Log System Messages 254
Configuring the Messages Included in the Log System 255
Value-added Services 257

Chapter 12

Gas Pump and Command Line Configuration 259

Gas Pump Configuration of the Router 260
Command Line Configuration 264
Command Line and Gas Pump Configuration File Commands 265
Example Config.txt Files 276
Example Config.txt File for a PPP Leased Line Link to the Internet from a CSU/DSU Port . . . 276
Example Config.txt File for a Frame Relay Link to the Internet from a WAN Port 279

Chapter 13

Troubleshooting 281

Troubleshooting Tools 281
Troubleshooting Procedure 282
Isolating the Problem 282
Typical Problems and Causes 287
General Problems 287
After making configuration changes, the router is restarting with the old configuration . . . 287
Console Port and Modem Problems 288
Modem is not detected on the console port 288
Cannot communicate with the router from a terminal connected to the console port 289
WAN Link Problems 290
CSU/DSU related errors 290
Leased line link will not start up 291
Data compression is configured but does not work 292
Abnormal X.25 SVC behavior 292
TCP/IP Related Problems 293
IP routing will not forward data traffic 293
Equipment will not boot over a WAN link 294
IPX Related Problems 295
IPX WAN link will not initialize 295
IPX routing will not forward data traffic 296
WAN Bridging Related Problems 297
Duplicated frames are seen on a network segment 297
Unable to bridge IPX data traffic 297
Unable to bridge IP data traffic 298
Long delays for bridged data traffic 298

Chapter 14

Recovery Mode 301

Overview 301
Network Boot Process using the Recovery Mode 302
Using Recovery Mode Manager in Intel Device View 303
Using the Recovery Mode from the Console Port 305
Resetting to Factory Default Configuration Using the Recovery Button 307

Appendix A

Limited Hardware Warranty 309

Appendix B

Technical Specifications 317

General Specifications 317
Hardware Specifications 318
LAN Ports 319
WAN Ports and Interface Cables 320
V.24 Interface and Cable 320
V.35 Interface and Cable 322
V.36 Interface and Cable 323
X.21/V.11 Interface and Cable 325
CSU/DSU Ports and Cables 326
Console Port and Supported Modems 327
Supported Modems 329
Supported Connections 331
Network and Bridging Protocols 332
WAN Protocols 334
Boot Sources 336
SNMP Management 336

Index 337

Support 354

Automated Support 354
Customer Support Technicians 354

Preface

Products covered

The following products are covered in this manual:

Product Name	Product Code
Intel Express 8210 Router	ER8210
Intel Express 8220 Router	ER8220
Intel Express 9530 Router	ER9530
Intel Express 9535 Router	ER9535

Product short names

The following terms are used within this manual to describe the products.

- Intel Express Router
- Express Router
- Intel Device View

Statutory Notices & Warnings

EMC caution

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

Use of shielded cables

To comply with EMC and FCC emission limits, use the shielded cables recommended by Intel Corporation.

Use unshielded cables only where explicitly allowed in the installation manual of the product in question.

Power supply warning

The Express Router does not have a main switch. Removing the power supply lead from the socket on the Express Router or disconnecting the power supply from the main supply socket disconnects the device from the main power. Therefore, both the socket on the Express Router and the power supply socket must be visible and easily accessible.

Power supply wiring color code

IMPORTANT!
The wires in the power supply cable provided with this equipment are color coded as follows:

Color	Connection
Green and yellow	Ground (Earth)
Blue	Neutral
Brown	Live

FCC Statements

FCC part 15 warning

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 operating 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.

FCC part 68 notice

This equipment complies with Part 68 of the FCC rules. Located on the equipment is a label that contains, among other information, the FCC registration number. If requested, this information must be provided to the telephone company.

This equipment cannot be used on the telephone company-provided coin service. Connection to Party Line Service is subject to State Tariffs.

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

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

If trouble is experienced with this equipment, please contact:

Intel Corporation—Jones Farm
2111 N.E. 25th Avenue
Hillsboro, Oregon 97124-5916
Telephone 503-696-8080

If the trouble is causing harm to the telephone network, the telephone company may request you to remove the equipment from the network until the problem is resolved.

It is recommended that the customer install an AC surge arrester in the AC outlet to which this device is connected. This is to avoid damaging the equipment caused by local lightening strikes and other electrical surges.

This equipment uses the following USOC jacks and codes

Interface	Facility Interface Code	Service Order Code	Jack Type
CSU/DSU T1	04DU9-BN	6.0N	RJ48C
CSU/DSU T1	04DU9-DN	6.0N	RJ48C
CSU/DSU T1	04DU9-1KN	6.0N	RJ48C
CSU/DSU T1	04DU9-1SN	6.0N	RJ48C
CSU/DSU T1	04DU9-1ZN	6.0N	RJ48C

Industry Canada Notice

IC CS-03 NOTICE (Canada)

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

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

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

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

Caution
Users should not attempt to make such electrical connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

The standard connecting arrangements (telephone jack type) for this equipment are CA81A, CA-A11, and CB-1D.

EEC Declarations

Safety

Intel Corporation declares that this product conforms with the requirements of the European Communities Directive of 73/23/EEC and 93/68/ECC on the harmonization of the laws of Member States for electrical equipment designed for use within certain voltage limits.

Electromagnetic Compatibility

Intel Corporation declares that this product conforms with the protection requirements of the Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility.

Telecommunications Terminal Equipment

Intel Corporation declares that this product conforms with the requirements of the Council Directive of 98/13/EEC on the approximation of the laws of the Member States concerning telecommunications terminal equipment, including mutual recognition of their conformity covering the following ports: WAN, WAN1, WAN2.

For UK use

IMPORTANT for use in the UK.
As the colors of the wires in the cable provided with this equipment may not correspond with the markings which identify the terminals in your plug, use the following procedure:

1. Check that the green and yellow wires are connected to the terminal marked with the letter E or the earth/ground symbol ⏚, or colored green and yellow.
2. Check that the blue wire is connected to the terminal which is marked with the letter N or colored black.
3. Check that the brown wire is connected to the terminal which is marked with the letter L or colored red.

Safety statement

The Safety Status of all interconnection points that are for the connection of other equipment is SELV (as defined by EN60950), or PELV (as defined by IEC364-4-41).

Line connections (UK only)

In order to meet the safety requirements of PSS/Digital Leased Line approval, it is important to ensure that the equipment is correctly installed and maintained. Connections to PSS/Digital Leased Lines must be made with the following cables:

Port Type	Data rate	Connector type	Cable Product Code
V.24	up to 19.2 Kbps	25-pin male D-sub	ER0001CB
V.35	up to 48 Kbps	34-pin female MIL-C-28748	ER0002CB
V.36	up to 64 Kbps	37-pin male D-sub	ER0003CB
X.21/ V.11	up to 64 Kbps	15-pin female D-sub	ER0004CB

Note The data rates given above indicate the data rate supported when transmitting across the respective branch system and do not necessarily reflect the maximum transmission speed supported by the equipment. For details of the port pin assignments, see Appendix "Technical Specifications", p. 317.

Branch systems (UK only)

The V.24 and V.35 interfaces are for connection only to a relevant branch system. For the purposes of approval, the port cables specified above constitute the relevant branch system.

The V.24 port is approved for PTO Service Category 1. The V.35 port is approved for PTO Service Category 2, ref. BS 6328 part 7: 1990.

Intended use

The intended use of this equipment is to provide data communications between remote sites via public or private telecommunication services. WAN ports are for connection to telecommunication services via an appropriate synchronous modem. CSU/DSU ports are for direct connection to T1 service.

All the features of the Express Router can be used within the United Kingdom.

Configuration

In order to fulfill its intended purpose, the Express Router must be configured to the user's needs. Setup of the Express Router using the Intel Device View Setup Wizard is described in the Quick Start Guide. Advanced Setup is described in this manual.

BCIQ (Taiwan) Declaration

BSMI Warning

警告使用者 ：
這是甲類的資訊產品， 在居住的環境中使用時，
可能會造成射頻干擾， 在這種情況下，使用者會
被要求採取某些適當的對策。

Approvals

Approvals

The Express Router complies with the following requirements:

Safety	UL 1950 CSA-C22.2 No. 950 IEC 950 EN 60950
Telecommunications	CTR 1 CTR 2 FCC part 68 IC CS-03
Emission	47 CFR part 15 Class A, EN 55022 Class A CISPR 22 Class A CNS 13438 Class A
Susceptibility	EN 55024 EN 50082-1
CE Mark	Yes

Wichtige Hinweise und Vorsichtsmaßnahmen

Erdung des Gerätes

Dieses Gerät muß Schutze des Fernmeldnetzes geerdet werden!

Farbkodierung der Leiter des Netzanschlußkabels

WICHTIG !
Dieses Gerät ist mit einem dreiadrigen Netzanschlußkabel ausgestattet. Die Leiter haben die folgende Farbkodierung:

Farbe	Leiter
Grün und Gelb	Erde
Blau	neutral
Braun	stromführend

Warnung zur Stromversorgung

Der Express Router besitzt keinen Ein/Aus-Schalter. Ein Entfernen des Stromkabels von dessen Anschluß im Express Router oder vom Stromnetz bewirkt ein Abschalten der Stromversorgung. Daher sollen sowohl die Buchse im Express Router und die Netzsteckdose gut sichtbar und leicht zugänglich angebracht werden.

Sicherheitsstand

Der Sicherheitsstand aller Verbindungsstellen des Macthbox Router, die dem Anschluss von weiteren Geräten dienen, ist SELV (Sicherheits-Kleinspannung) (entsprechend der Definition von EN60950) und PELV (gemäß IEC364-4-41).

Notes Statutaires et Avertissements

Mise à la terre

Cet appareil doit être relié à la terre pour protéger le réseau de télécommunications.

Code couleur des conducteurs du cordon secteur

IMPORTANT !
Les couleurs du cordon secteur fourni avec cet appareil correspondent au code suivant:

Couleur	Branchement
Vert/Jaune	Terre
Bleu	Neutre
Brun	Phase

Alimentation secteur

ATTENTION!

Le Express Router ne possède pas d'interrupteur secteur. Pour débrancher cet équipement, il faut retirer le cordon d'alimentation soit du connecteur situé sur le Express Router soit de la prise secteur. Il est donc important de garder ces deux connecteurs bien visibles et faciles d'accès.

Déclaration de sécurité

Tous les points d'interconnexion du module de Express Router, d'enceinte pour le branchement d'autres équipements est SELV (comme défini par IEC950/EN60950) et PELV (comme défini par IEC364-4-41).

Bezpečnostní výstraha

Výstraha pro dodávku proudu

Prístroj musí byt umistěn v blízkosti sit'ové zásuvky. K odpojení přistroje od sítě slouží vidlice sít'ového přívodu.

This manual uses the following conventions:

Item	Convention
Menu items, buttons, parameters	These are written in Courier typeface, having the same nomenclature as on screen.
Accessing submenus	Indicated by ">" between each menu item, For example, Device>Install.
WAN port and WAN	The phrase "WAN port" is used when referring specifically to the port designated as a WAN port on the router (for example, "Connecting the WAN port"). "WAN" is used as a general term referring to Wide Area Network (for example, WAN services)
"Link" and "Connection"	For the purposes of this manual, the words Link and Connection have the same meaning.

Acronyms

ARP	Address Resolution Protocol
BCP	Bridging Control Protocol
BOOTP	Boot Protocol
BPDU	Bridging Protocol Data Units
CBC	Cipher Block Chaining
CCITT	Comité Consultatif International Télégraphique et Téléphonique
CCP	Compression Control Protocol
CHAP	Challenge Handshake Authentication protocol
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSU	Channel Service Unit
DCE	Data Circuit-terminating Equipment
DE	Discard Eligibility
DHCP	Dynamic Host Control Protocol
DLCI	Data Link Connection Identifier
DLCMI	Data link Connection Management Interface (also called LMI)
DMZ	Demilitarized Zone
DNS	Domain Name Service
DRAM	Dynamic Random Access Memory
DSU	Data Service Unit
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
ECP	Encapsulation Control Protocol

FCC	Federal Communications Commission
FR	Frame Relay
FRI	Frame Relay Interface
FTP	File Transfer Protocol
GNS	Get Nearest Server
HDLC	High-level Data Link Control
HTTP	HyperText Transfer Protocol
ICMP	Internetwork Control Message Protocol
IEC	International Electrical Commission
IGMP	Internet Group Management Protocol
IMAP4	Internet Message Access Protocol 4
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPX§	Internetwork Packet Exchange§
IPXCP	Internetwork Packet eXchange Control Protocol
ISP	Internet Service Provider
LAN	Local Area Network
LAPB	Link Access Procedure, Balanced
LCP	Link Control Protocol
LMI	Link Management Interface
MIB	Management Information Base
MROUTD	Multicast Route Daemon
NAT	Network Address Translation
NFS	Network File Server
PAP	Password Authentication Protocol
PDN	Public Data Network
PING	Packet InterNetwork Groper function
POP3	Post Office Protocol 3
PPP	Point-to-Point Protocol
PVC	Permanent Virtual Circuit
RIP	Routing Information Protocol
RSVP	Resource ReSerVation Protocol
Rx	Receive
SAP	Service Access Point
SELV	Safety Extra Low Voltage
SIMM	Single In-line Memory Module
SMPT	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPX	Sequenced Packet Exchange
SVC	Switched Virtual Circuit
TCP	Transfer Control Protocol
TFTP	Trivial File Transfer Protocol
TNV	Telecommunications Network Voltages
Tx	Transmit

UDP	User Data Protocol
WAN	Wide Area Network

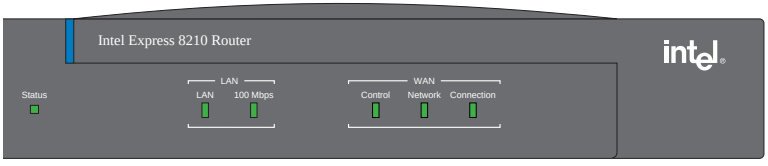
1 Introduction to the Intel® Express Router

Hardware Overview

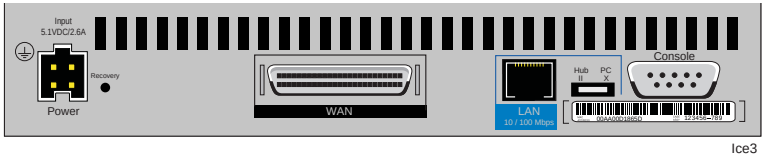
Intel® Express 8210 front and back panels

The following shows the front and back panels of the Intel Express 8210 Router.

Front Panel (ER8210)



Back Panel (ER8210)



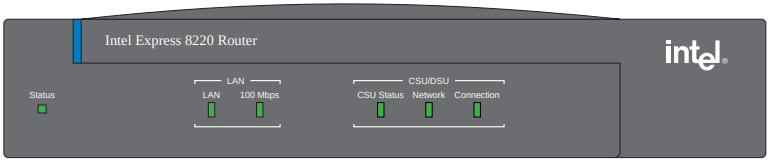
Ice3

Ports: 1 WAN, 1 10/100 Base-T LAN, 1 Console

Intel Express 8220 Router front and back panels

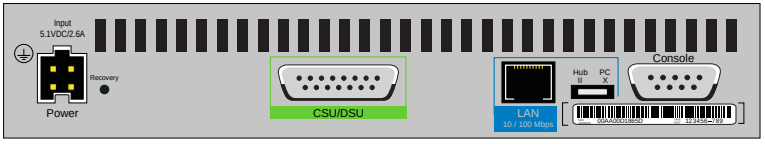
The following shows the front and back panels of the Intel Express 8220 Router.

Front Panel (ER8220)



Ice2

Back Panel (ER8220)



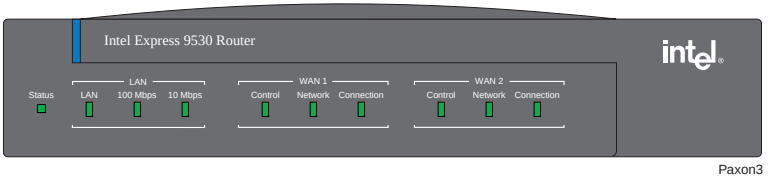
Ice4

Ports: 1 CSU/DSU, 1 10/100 Base-T LAN, 1 Console

Intel Express 9530 Router front and back panels

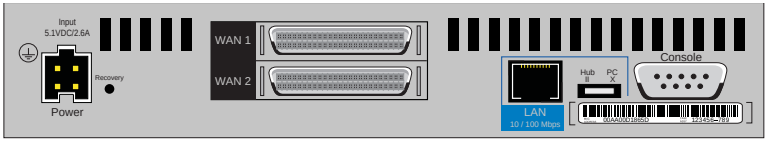
The following shows the front and back panels of the Intel Express 9530 Router.

Front Panel (ER9530)



Paxon3

Back Panel (ER9530)



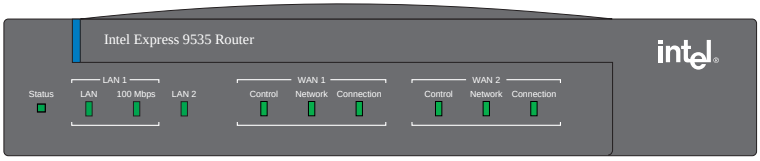
Paxon1

Ports: 2 WAN, 1 10/100 Base-T LAN, 1 Console

Intel Express 9535 Router front and back panels

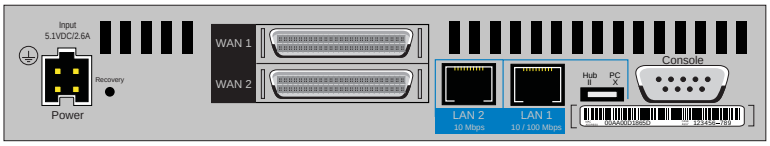
The following shows the front and back panels of the Intel Express 9535 Router.

Front Panel (ER9535)



Paxon8

Back Panel (ER9535)



Paxon6

Ports: 2 WAN, 1 10 Base-T LAN, 1 10/100 Base-T LAN, 1 Console

Port descriptions

The following table provides brief descriptions of the ports found on the Express Routers.

Port	Description
CSU/DSU	A built-in CSU/DSU provides a direct connection to a T1 interface through a DB-15 type connector.
WAN	Accommodates X.21/V.11, V.24, V.35 or V.36 connections by using special adapter cables. The cable required for your installation must be ordered separately.
LAN or LAN1 (10/100 Mbps)	An RJ-45 connector providing an Ethernet interface for the direct connection to a 10Base-T or 100Base-T local area network. The HUB/PC switch terminates the port for connection to either a PC or network hub or switch.
LAN2 (10 Mbps)	An RJ-45 connector providing an Ethernet interface for the direct connection to a 10Base T local area network.
Console	A 9-pin serial connector provides direct access to the on-board Local Management from a VT100-compatible terminal, or it can be used for wide area network access through a dial-up modem.

Recovery Button

The Recovery button is used to place the router in Recovery Mode or reset the router to the factory default configuration. See Chapter 14 “Recovery Mode”, p. 301 for details.

LED Descriptions

Status LED

The following describes the Status LEDs.

LED	Color	Indication
Status	green, steady	Router is operational.
	green, blinking	Router is set to factory default, awaiting configuration.
	orange, steady	Diagnostics error, router is operational.
	orange, blinking	Router is in Recovery Mode.
	red	Fatal error, router is not operational.
	off	Power is off.

LAN LEDs

The following describes the LAN LEDs.

LED	Color	Indication
LAN, LAN1, LAN2	green, steady	Port is operational but no data activity.
	green, blinking	Data activity on the LAN.
	orange, steady	Port is down or disabled.
	orange, blinking	Ethernet collisions on the port.
100 Mbps	green, steady	Ethernet LAN is operating at 100 Mbps
	off	Ethernet LAN is operating at 10 Mbps.
10 Mbps	green, steady	Ethernet LAN is operating at 10 Mbps.
	off	Ethernet LAN is operating at 100 Mbps.

WAN Port LEDs

The following describes the WAN (1 or 2) port LEDs.

LED	Color	Indication
Control	green, steady	Modem or CSU/DSU connection established.
	orange, steady	Modem or CSU/DSU connection not established.
	red	Error connecting to modem or CSU/DSU.
Network	green, steady	Connection to the network established.
	orange, steady	No connection to the network, WAN port is disabled.
	orange, blinking	Attempting to connect to the network.
	red	Error connecting to the network.
Connection	green, steady	WAN connection established, no data activity.
	green, blinking	Data activity on the port.
	orange, steady	No call connected, WAN connection not established.
	orange, blinking	Attempting to establish a WAN connection.
	red	Error establishing the WAN connection.

CSU/DSU Port LEDs

The following describes the CSU/DSU port LEDs.

LED	Color	Indication
CSU Status	green, steady	Connection to the CSU of the data network switch is established.
	green, intermittently blinking orange	Connection to the CSU of the data network is established. The orange blinks correspond to errors detected by the CSU.
	orange, steady	Attempting to establish connection to the CSU on the data network switch. Corresponds to a CSU Yellow alarm.
	orange, blinking	Testing the line.
	red, steady	Error, unable to connect to the CSU on the data network switch. Corresponds to a Red, Blue or Out-of-frame Alarm.
Network	green, steady	Connection to the data network switch is established.
	orange, steady	No connection to the data network switch; CSU/DSU port is disabled or not configured.
	orange, blinking	Attempting to connect to the data network switch.
	red, steady	Error; unable to connect to the data network switch.
Connection	green, steady	WAN connection established, no data activity on the port.
	green, blinking	Data activity on the port.
	orange, steady	No call connected, WAN connection not established.
	orange, blinking	Attempting to establish the WAN connection.
	red	Error establishing the WAN connection.

All LEDs Flashing

All LEDs flashing in sequence indicates that the router is loading firmware.

Features of the Intel Express Router

Management

Intel Device View

Intel Device View is a network device management software supplied with the router on a CD-ROM and is the recommended management tool. Intel Device View provides a graphical interface for the installation, configuration, and monitoring of the router, and other Intel network devices, from a PC running Windows§95/98/2000 or Windows NT§. Three installations options are available:

Intel Device View for Windows

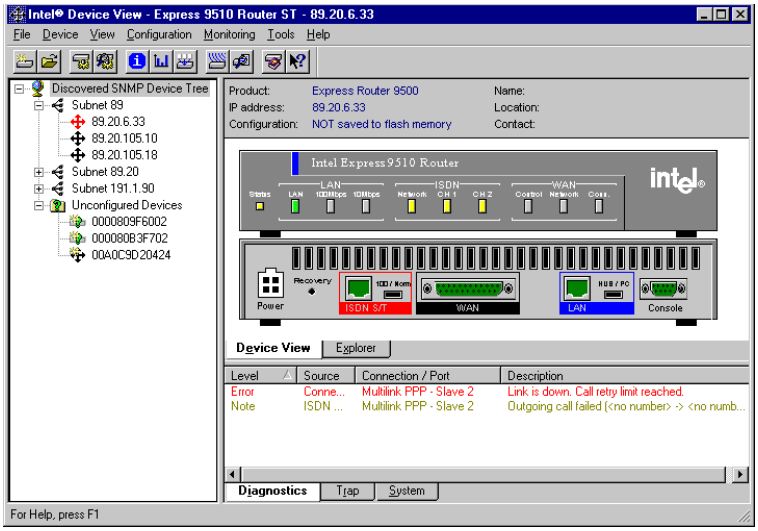
Intel Device View for Windows is installed directly on a PC and allows you to manage the router and other network devices from that PC.

Intel Device View for Web

Intel Device View for Web is installed and hosted on a Web server. This allows you to manage the Express Router and other Intel network devices on the network from any client PC using a supported Web browser.

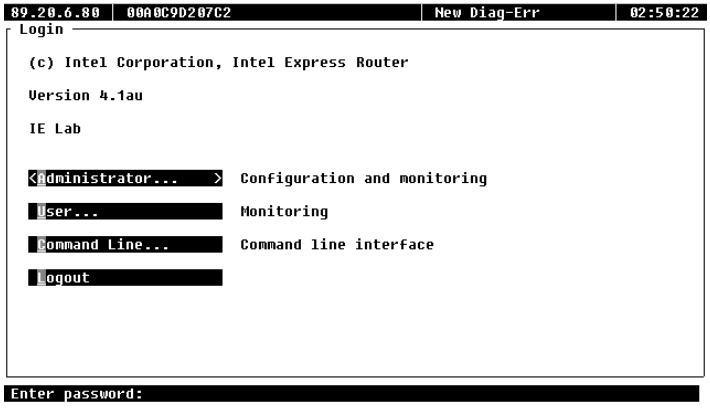
Intel Device View as a Plug-in

Installing Intel Device View as a plug-in provides Intel network device support for Hewlett Packard OpenView§, Tivoli NetView§ or Intel LANDesk® Network Manager. For information, see the documentation for these programs.



Local Management

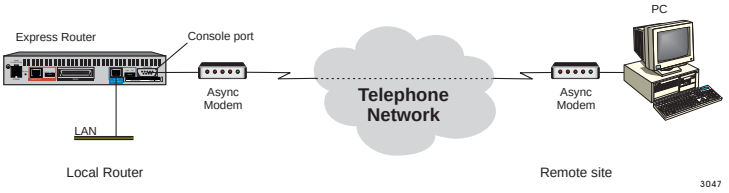
Local Management is an on-board management application that supports full monitoring and configuration capabilities.



You can access Local Management in the following ways:

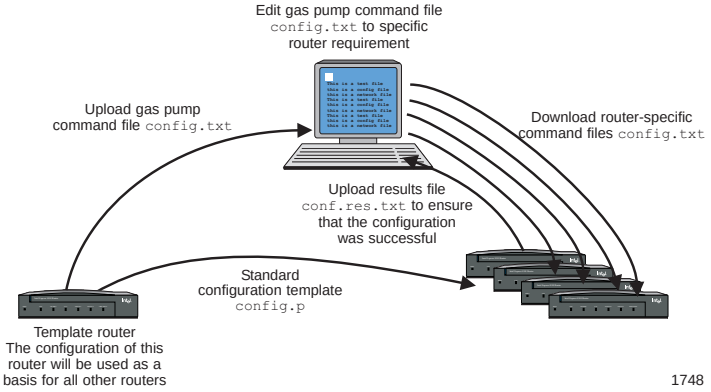
- From Intel Device View, click `Telnet` from the Tools menu.
- Start a Telnet session to the router's IP address from any terminal on the router's LAN or WAN.

Use a VT100-compatible terminal or PC running emulation software connected to the console port, either directly or via an asynchronous modem dial-in connection (illustrated).



Command line interface and multiple router configuration using TFTP

A command line interface is available from Local Management that provides limited configuration. Command line allows you to configure a number of routers based on the configuration of single router using Trivial File Transfer Protocol (TFTP). See Chapter 12 for details.



CSU/DSU T1 Services

CSU/DSU Port

The CSU/DSU port on the Express Routers provides a direct interface to a T1 line from a built-in CSU/DSU. The CSU/DSU port supports full T1 or fractional T1 service to a Frame Relay or X.25 network, or a PPP leased line connection.

T1 service

T1is a full-duplex digital signal operating at a data rate of up to 1.536 Mbps. The signal is divided into 24 channels or time slots operating at 64 Kbps or 56 Kbps.

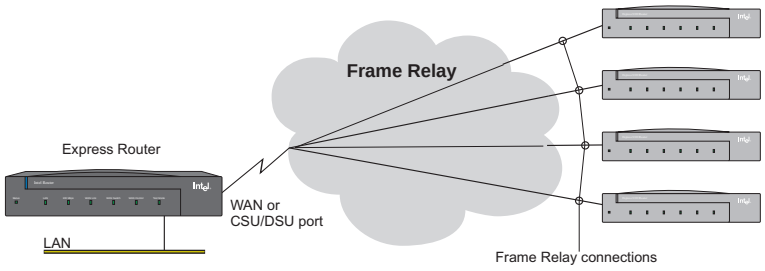
Fractional T1

Fractional T1 allows you to purchase and use less than full T1 service. With fractional T1, you can subscribe up to 23 channels at 56 Kbps or 64 Kbps (depending on your service) to get the desired bandwidth.

Frame Relay Services

Frame Relay Overview

Frame Relay service is available for use through WAN and CSU/DSU ports on the Express Router. Frame Relay provides LAN interconnections over a WAN at rates of up to 2.048 Mbps, and allows multiple simultaneous data sessions (logical connections) across a single physical connection (see “Supported Connections”, p. 331).



Frame Relay data compression

Data compression is available when communicating over Frame Relay connections which can improve the throughput. Data compression is hardware-based and offers maximum possible compression at the line speeds supported by the router. Data compression is done us-

ing Frame Relay compression (FRF.9) or a proprietary standard to provide compatibility with older Intel routers. The correct compression algorithm is automatically determined by negotiation with the remote router over the Frame Relay connection.

Data compression uses the Stac§ algorithm, and typical compression rates of 4:1 can be expected for ASCII files.

Default Frame Relay set up

Frame Relay service is configured by default for WAN and CSU/DSU ports. The router automatically detects the Frame Relay switch type (DLCMI) and the Frame Relay connections (DLCIs) in your Frame Relay subscription. The router configures the detected Frame Relay connections with default routing of IP (RIP-1) and IPX§. This allows you to remotely configure your router over a Frame Relay connection after the router hardware is installed.

Flow control

The Express Router supports a number of features to facilitate the effective transmission of data over multiple Frame Relay connections in periods of excessive date traffic:

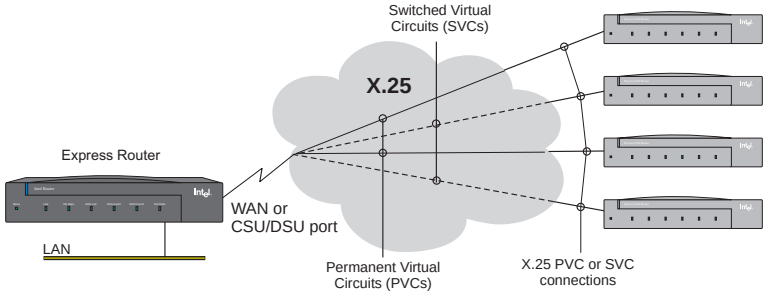
- Congestion avoidance through Backward Explicit Congestion Notification (BECN)
- Prioritizing connections by configuring parameters such as Committed Information Rate (CIR), Committed Burst (Bc), Excess Burst (Be), and bandwidth weight.
- A proprietary protocol for exchanging line speeds between routers to ensure the router does not transmit more traffic than the remote router is able to receive.

For details on flow control features, refer to the section in Chapter 6, “Flow Control”, p. 110, or see the Reference Manual.

X.25 Services

X.25 overview

X.25 is available for use on WAN and CSU/DSU ports of the Express Router. X.25 offers the interconnection of LANs over public or private X.25 networks.



Connections across X.25 networks are made using virtual circuits (logical channels). X.25 logical channels can be either Permanent Virtual Circuits (PVCs) or Switched Virtual Circuits (SVCs). PVCs offer connections that are permanently available and are similar to a leased line. SVCs are connections that are only established when a transfer request is initiated and are cleared as soon as the data has been transferred. Multiple X25 SVC connections can be configured on any port (see “Supported Connections”, p. 331).

X.25 data compression

Data compression is available when communicating over X.25 connections, to improve the throughput on connection speeds of up to 128 Kbps. Typical compression rates of 4:1 can be expected for ASCII files.

X.25 reverse charges

Reverse charges can be used to transfer the costs of operation for a connection to a specific location.

For example, if someone working from a remote site needs a connection to a central office, the costs of operation for the connection can be transferred to the central office using reverse charges. When the

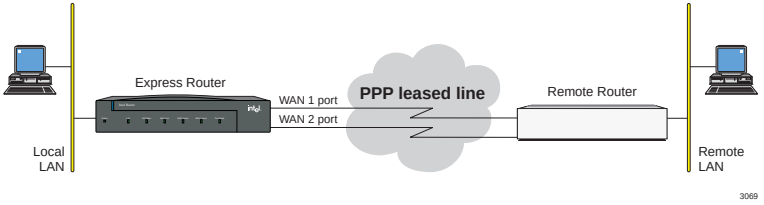
remote site needs to communicate with the central office, the remote site router will call in to the central office router which then calls the remote site back.

Note Reverse charge services must be available in your X.25 service subscription before they can be used by your router; otherwise these requests will be ignored.

PPP Leased Line Multilinks

PPP leased line multilink

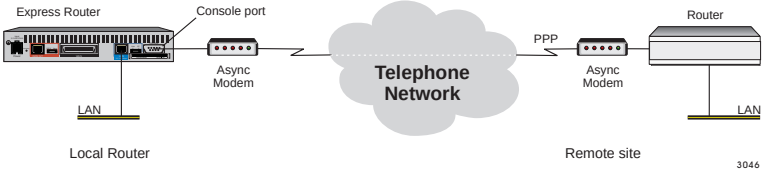
The Intel Express 8210 Router supports a PPP Multilink using a leased line connection off each WAN port. The individual leased lines must operate at the same transmission rate to create a multilink. In effect, the PPP Multilink doubles your transmission rate.



PPP Dial-up Modem Connections

PPP Dial-up connections

The console port of the router supports dial-up PPP connections over a normal telephone network via an asynchronous modem. All the facilities offered by PPP connections are available, such as data compression, CHAP/PAP, and callback.



Point-to-Point Protocol (PPP)

PPP overview

PPP is a standardized data connection level encapsulation protocol for communicating over leased lines, dial-up modem connections, and Internet Tunnels. PPP verifies, to some extent, that the PPP configurations in the two routers over the connection are consistent. The features available for communicating over PPP connections include:

- Data compression
- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Call-back (ISDN and dial-up modem connections only)

Data compression

Data compression can improve throughput on the PPP connections. Data compression is hardware-based and offers maximum possible compression at the line speeds supported by the router. The compression technique is based on the Stac§ algorithm and typical compression rates of 4:1 for ASCII files can be expected.

In most cases, the router autodetects the standard compression modes, **Sequenced Number Mode** and **Extended Mode** (Microsoft-compatible).

Password Authentication Protocol (PAP)

PAP uses simple password exchange to validate devices over a PPP connection and to respond to authentication requests from other devices. PAP is an effective way of ensuring that only communications from authorized devices are accepted over a PPP connection.

Challenge Handshake Authentication Protocol (CHAP)

CHAP can be chosen as an alternative to PAP to validate devices over a PPP connection before communications are permitted. CHAP is more secure than PAP as CHAP never actually transmits the password over the connection. CHAP is therefore resistant to attempts to obtain the password by monitoring the PPP connection. The use of CHAP is recommended over PAP.

Call-back

Call-back is available for PPP connections over dial-up modem connections. Call-back can be used to transfer the costs of operation for a connection from this location or to a remote location. For example, if someone working from home needs a connection to an office, the costs of operation for the connection can be transferred to the office

by using callback. When the home connection needs to communicate with the office, they call to the office router which then calls them back

PPP Callback

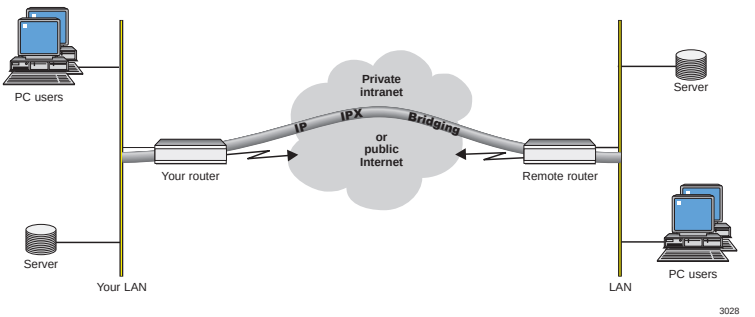
When using PPP callback, a device requesting callback must establish the connection to request callback. This means that some costs will be incurred at the requesting site, even though most of the costs will be transferred to the remote site

PPP Call-back is available in proprietary mode (standards-based) for compatibility with older Intel Routers, and standard RFC 1570 mode. which is compatible with the callback standard from Microsoft§.

Internet Tunnels

Internet routing (Internet Tunnels)

Internet Tunneling is available in the Express Router for routing data via the public Internet.



Routing data via the Internet can be very cost-effective when compared with the costs of routing via conventional direct wide area network connections. The costs of operation consist of only the subscription to an Internet service provider (ISP), and the costs (if any) of local calls to your ISP. This can offer substantial savings over routing data directly via traditional service connections.

Network and Bridging Services

Network layer services

The Express Routers provides the following network layer services:

- IP routing (RIP-1, RIP-2 and static routes)
- Novell routing (IPX/SPX RIP/SAP and IPX static routes)
- WAN bridging, for forwarding data that cannot be routed.

IP routing

The IP routing services implemented in the router include the Transfer Control Protocol (TCP), Routing Information Protocol (RIP-1 and RIP-2), BootP, Address Resolution Protocol (ARP), subnets, control and management of IP connections using ICMP (Internetwork Control Message Protocol) and the establishment of static routes.

Firewall and IP Filters

The Express Router implements comprehensive IP packet filtering to restrict communications between networks and hosts and to eliminate or minimize unwanted traffic. These filters provide the basis for creating a firewall. Features of IP filtering and firewall protection are:

Static and Stateful Filters

The router offers two types of filters, static and stateful. Static filters can discard or pass data that meets criteria set by the filter. These filters are considered static because they do not change their state, that is, they are always active. Stateful filters are dynamic filters based on the principles of Stateful Inspection. These filters provide time-limited access through your firewall for packets that meet the filter criteria. Stateful filters remember the source and destination addresses and port numbers of a connection and use this information to ensure incoming data is from a valid destination. Stateful filters offer a much tighter security than static filters and are preferred when creating a firewall.

SYN Flood Protection

TCP SYN flood attacks can be damaging to Internet services such as Web servers or FTP servers. With stateful filter, the router can protect these services on your network using the SYN Flood Protection feature.

Port to Application Mapping

Port to application mapping allows you to use non-standard port numbers for FTP and HTTP services when filtering using stateful filters.

Triggered IP RIP

Triggered RIP is available for use over WAN connections. For on-demand type (dial-up) connections, this prevents connections from being brought up just to send routing information through RIP. When using triggered RIP, routing information is only exchanged when the connection comes up or when a network topology change is detected. This can considerably reduce RIP update overheads.

OSPF routing

OSPF (Open Shortest Path First) routing protocol is a licensed software feature that you can purchase to upgrade your router. OSPF is based on a link-state routing protocol which makes it preferable to RIP, especially in large networks.

Dynamic IP Address Assignment

Dynamic IP Address assignment can be used over PPP leased lines to obtain addresses allocated from a remote device (usually an Internet Service Provider). Whenever the connection is brought up, the router will request an IP address from the remote device. If an IP address is given by the remote device, the router will use that address for the duration that the connection is up.

IP Multimedia protocols

The following IP multimedia features are implemented in the Express Router:

Resource Reservation Protocol (RSVP)

The IP Resource Reservation Protocol (RSVP) is a protocol used by multimedia applications to provide quality of service for video and communications. RSVP allows bandwidth over WAN connections to be reserved for applications which require a guaranteed data delivery for satisfactory performance.

IP Multicasts

IP Multicasts are typically used by multimedia applications to communicate with multiple remote devices simultaneously. IP Multicasts are supported using MROUTD specifications that use the Internetworking Group Multicast Protocol (IGMP) on the LAN and Distance Vector Multicast Routing Protocol (DVMRP) to communicate IP Multicasts routes between routers.

IP Multicast Tunneling

IP Multicasts can only be transmitted between routers which support IP Multicast routing (using DVMRP). If intermediate routers do not support DVMRP, IP Multicast Tunnels can be established to allow IP Multicasts to bypass them to maintain the IP Multicast network topology.

IP Network Address Translation (NAT)

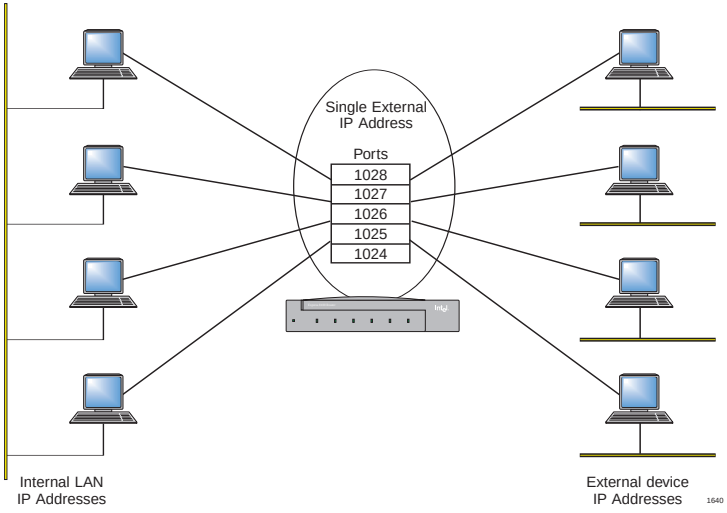
IP Network Address Translation (NAT) is available to translate internal LAN addresses to external addresses. NAT is very useful in many IP applications including:

- Connecting your LAN to the Internet

  The Internet requires the use of public IP addresses that are usually assigned by Internet service providers. NAT can be used to translate private (non-public) IP addresses to official public addresses that can be used on the Internet.

- Making one or a few IP addresses available to all devices on the LAN

  NAT allows a single IP address to be used by many devices on the LAN at the same time. For example, ISPs typically assign a single public Internet IP address to a site. NAT maps internal LAN IP addresses to different TCP ports of the single public IP address. This makes the single IP address available to many devices on your LAN simultaneously.



- Connecting two networks together that have the same IP network address.

IPX filters

Comprehensive IPX routing filters are implemented in the router. These allow access restrictions to be defined for communications between networks and hosts, and to eliminate unnecessary or unwanted network traffic.

Novell IPX routing

The implementation of IPX is compatible with Novell's implementation. Novell supports different types of Ethernet frames (packets)—IPX packets are encapsulated into the frame types supported by NetWare§ servers. To ensure compatibility with routers from other manufacturers, the Novell IPX WAN2 Protocol is supported via both numbered and unnumbered WAN connections.

IP and Novell IPX static routes

Static routes are available for both IP and IPX (static routes and services). If only a limited number of networks are accessed over a WAN connection, static routes to the remote networks can be established to eliminate the routing information sent by the dynamic routing protocols (IP RIP, IPX RIP and SAP). By eliminating the network overheads, the available connection bandwidth is maximized for data traffic and the costs of operation are minimized.

WAN bridging (data link layer service)

Where a protocol is non-routable or the native routing protocol is not supported, the router uses efficient bridging services to forward data. The Spanning Tree§ Algorithm is supported to achieve the most efficient bridging routes.

Controlled bridging functions allow you to forward packets addressed to defined destinations, from defined sources and for defined Ethernet frame types. Bridge learning can also be disabled. These features offer secure bridging by bridging between authorized stations. It is a cost-effective use of WAN connections by only bridging essential services.

Dynamic Host Control Protocol (DHCP) Server

DHCP Server

DHCP (Dynamic Host Control Protocol) is an industry protocol used to dynamically assign IP addresses to network devices. The Express Router provides a built-in DHCP server that gives the router the ability to automatically assign:

- an IP address, including a subnet mask and gateway address
- a DNS (Domain Name System) server address
- WINS (Windows§ Internet Name Service) server address.

The DHCP server provides an efficient way to assign and manage your IP address allocation.

Router Factory Default Setup

Express Router Factory Default Setup

The Express Router is supplied with the following default setup, depending on the port types available for your router.

Port	Parameter	Default Setting
General	IP Routing	Enabled using RIP-1
	IPX Routing	Disabled
	WAN Bridging	Disabled
LAN	IP Address	192.0.2.1
	Network Mask	255.255.255.0
LAN1	IP Address	192.0.2.1
	Network Mask	255.255.255.240
LAN2	IP Address	192.0.2.17
	Network Mask	255.255.255.240
WAN, WAN1	WAN Protocol	Frame Relay
	Management Interface (DLCMI)	Autodetected
	Baudrate	Autodetected
	Frame Relay Connections	Automatically configured for each autodetected Data Link Connection Identifier (DLCI) available in your subscription.
	IP Routing	RIP-1
	IPX Routing	Enabled using the IPX WAN Protocol
WAN2	WAN Protocol	PPP leased line

Port	Parameter	Default Setting
CSU/ DSU	Channel Selection	On
	Channel Bandwidth	64 kps
	Line Coding	B8ZS
	Timing Mode	Network (Loop Timing)
	Line Build Out	0 dB
	Framing Format	ESF
	Receiver Sensitivity	Norm
	Disable ANSI PRM	No
	WAN Protocol	Frame Relay
	Management Interface (DLCMI)	Autodetected
	Baudrate	Autodetected
	Frame Relay Connections	Automatically configured for each autodetected Data Link Connection Identifier (DLCI) available in your subscription.
	IP Routing	RIP-1
	IPX Routing	Enabled using the IPX WAN Protocol
Console	Console port mode	Console mode

By default, data compression is negotiated between the connections if it is available in the remote devices.

2 Installation

Warnings

Important!

Before you proceed with the installation procedure given in this chapter, you must read the Statutory Notices and Warnings provided at the beginning of this User Guide.

Wichtig!

Bevor Sie mit der Installation des Gerätes beginnen, sollten Sie unbedingt die wichtigen Hinweise und Vorsichtsmaßnahmen, die am Anfang dieser Bedienungsanleitung beschrieben sind, sorgfältig durchlesen.

Important!

Avant de continuer avec la procédure de l'installation dans ce chapitre, il faut lire les Notes importantes et les Avertissements au début de ce clavier.

Product Parts

Standard product parts

The router package contains the following components:

- Intel Express Router
- power cable

- LAN connection cable (blue)
- CSU/DSU TI cables (green) - supplied with the ER8220 router only
  - DB15 to RJ48C cable (standard)
  - DB15 to RJ48C adapter cable
- HDSL2 connection cable (red) - supplied with the ER9545 router
- Console port terminal cable (DB9 to DB9)
- CD-ROM containing:
  - Intel Device View
  - a backup copy of the router firmware
  - the Reference Manual, User Guide (this manual) and Quick Start for the router in PDF format
  - Intel Device View User Guide in PDF format
  - Intel Express Router Interoperability Guide
  - Acrobat§ Reader for reading the on-line manuals
  - Microsoft Internet Explorer§ version 5.0
- Quick Start
- User Guide
- Late-breaking News

Optional product parts

The following product parts are ordered separately as needed.

Part Description	Product Code
WAN port cables	
V.24 (RS-232) DTE interface cable	ER0001CB
V.35 DTE interface cable	ER0002CB
V.36 (EIA-449) DTE interface cable	ER0003CB
X.21/V.11 DTE interface cable	ER0004CB
CSU/DSU T1 cables	
DB15 to DB15	ER0005CB

Installation Procedure

Quick installation instructions

For quick installation instructions, use the Quick Start guide included with the router.

Important

The Intel Express Router must be installed by authorized technical personnel. It must be handled with great care at all times, and must not be exposed to violent shock or any other influences that may result in damage and possible functionality failures. Intel cannot be held responsible for any damage arising as a result of incorrect handling or installation.

Main supply warning

IMPORTANT!

The router does not have a main power switch. Removing the power supply unit lead from the socket on the router disconnects the router from the power supply. Therefore, the socket on the router and the main supply socket should be easily accessible.

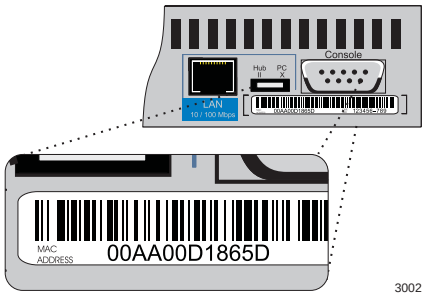
Preparation

Read the Late-breaking News

The Late-breaking News document included with the router contains essential information regarding the router operation (such as limitations or known errors). This is information made available after this manual was completed. Read this document before you begin to install the router.

Identify the MAC address

Make note of the MAC address assigned to the router which is printed on the label next to the LAN port. The MAC address is in the format `00123456789A` (12 hexadecimal numbers).



This is the MAC address assigned to the LAN or LAN1 (10/100Mbps) port. For routers having two LAN ports, the LAN2 port has a MAC address which is one unit greater than the printed MAC address. Using the MAC address in the diagram as an example, the MAC address of the LAN2 port is 00AA00D1865E.

Intel Device View Install Wizard uses the MAC address to identify the router during initial configuration.

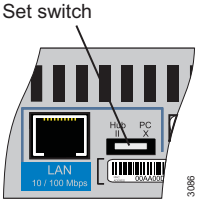
Connecting the Intel Express Router

Connecting to the Local Area Network (Ethernet)

To connect the LAN or LAN1 port (10/100Mbps)

To connect the 10/100 Mbps LAN port (labelled either LAN or LAN1 depending on your router):

1. Connect the port to a local network (such as a hub or Ethernet switch) or Ethernet port of a PC using the blue LAN cable provided.
2. Set the HUB/PC switch next the LAN port to the proper position.



Set the switch to	When connecting to
HUB	a local network via an Ethernet device such as a hub or switch.
PC	a PC

The blue LAN cable is a straight-through cable. The switch eliminates the need for a crossover cable.

To connect the LAN2 port (10Mbps)

To connect the 10 Mbps LAN2 port to an Ethernet network, use one of the following 10 Base-T Ethernet cables (RJ-45 to RJ45):

- To connect to a hub or Ethernet switch, use a straight-through cable.
- To connect to a PC, use a cross-over cable.

Note These cables are not included with the router.

Connecting the WAN Port

Connecting the WAN port

A WAN port on the Express Router connects to a leased line, Frame Relay, or X.25 service through an external synchronous modem or CSU/DSU unit (user supplied). The interconnecting cable between the router and the modem depends on the modem interface and is ordered separately as required (see “Optional product parts”, p. 24).

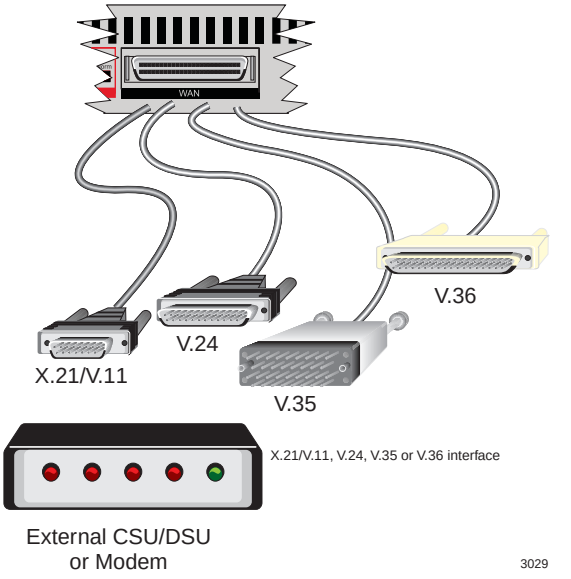
Equipotential bonding requirement

The WAN cables used to connect to the modem or CSU/DSU are shielded. If the modem is Class I equipment (grounded), there is a risk of circulating loop currents through the shield and the pin 1 wire in the cable. To avoid this risk, the router and modem must be connected to main outlets which comply with the requirements for equipotential bonding according to IEC 364-4-41, ITU-T/CCITT K.31 or similar local/national regulations.

To connect a WAN port

To connect a WAN port of the router:

1 Use the appropriate black WAN connect cable to connect the WAN port of the router to an external synchronous modem or CSU/DSU.



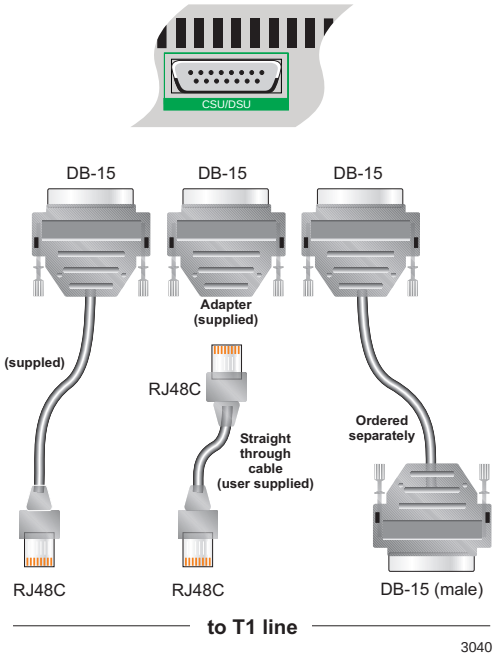
2 Make sure the router and the modem or CSU/DSU are grounded by their respective main supply connections and the electrical potential between the router and the modem or CSU/DSU is zero before you apply power to the router. Otherwise, establish a separate wire connection between the router and the modem or CSU/DSU. The router is equipped with a grounding screw located on the back panel, indicated by ⏚.

3 Check the modem is properly connected to the WAN service provided.

Connecting the CSU/DSU Port to a T1 Service

To connect a CSU/DSU port

The CSU/DSU port of an Express Router supports direct connection to a T1 line for PPP leased line, Frame Relay and X.25 service. Connect the CSU/DSU port to the T1 line using one of the cable combinations shown. The CSU/DSU cables supplied with the router are green.



Connecting a Dial-up Modem to the Console Port

Supported modems

The console port supports the installation of an asynchronous modem for PPP dial-up connections over a normal telephone network. A number of modem types can be configured for use. Refer to “Supported Modems”, p. 329 for details.

Note If you are not using a supported modem, additional configuration for the modem may be necessary. See Chapter 6, “Configuring the Console Port for the Modem and the PPP Dial-up Links”, p. 124. The compatibility of non-supported modems with the Express Router is not guaranteed.

Equipotential bonding requirement

If the modem is Class I equipment (grounded), there is a risk of circulating loop currents through the shield and the pin 1 wire in the cable. The router and modem must be connected to main outlets which comply with the requirements for equipotential bonding according to IEC 364-4-41, ITU-T/CCITT K.31 or similar local/national regulations.

To connect a dial-up modem to the Console Port

To connect an asynchronous modem to the console port:

1. Before applying power to the router or modem, make sure the router and the modem are grounded by their respective main supply connections and the electrical potential between the router and the modem is zero. Otherwise, install a separate ground wire between the router and the modem. The router is equipped with a grounding screw located on the back panel, indicated by ⏚.
2. Connect the asynchronous modem to the console port of the router using the cable supplied with your modem.
3. Connect the modem to your telephone network as required.

Connecting the Console Port to a VT100-compatible Terminal or PC

Connecting a VT100-compatible terminal

The console port of the router supports the connection of a VT100-compatible terminal or PC running emulation software such as HyperTerminal§(HT). The terminal can be used for configuration and monitoring purposes.

To connect to the Console Port

To connect a VT100-compatible terminal or PC to the console port:

1. Using the supplied console port terminal cable (DB9 to DB9), connect the console port of the router to the VT100-compatible terminal or serial (COM) port of a PC.
2. If connected to a PC, start the terminal emulation software.

3 Set the terminal emulation parameters.

Parameter	Setting
baud	9600
data bits	8
parity	none
stop bits	1
flow control	none

For instructions on how to set the parameters, consult the documentation for the emulation software.

Power Up the Router

To connect the router power supply

To connect the router power supply:

1 On the back of the router, connect one end of the power supply and cable assembly to the power socket.

2 Connect the other end of the power cable to a 100-250 VAC power source.

Since there is no power switch for the router, the router turns on when the power source is on. The Status LED lights up when the power is applied.

Software Installation

Installing Intel® Device View

System information for Intel Device View

The system information for the installation and use of Intel Device View:

Recommendations for Intel Device View for Windows§:

- PC with a Pentium® processor 120 MHz equivalent or faster, performance level or better, 32MB RAM, and an installed network adapter.
- SVGA color display with a minimum resolution of 800 x 600 (1024 x 768 recommended) and 256 colors.
- Windows§ NT§ workstation or server version 4.0 (service pack 3 or higher recommended), Windows 95 (release A: service pack 1 or B: OEM 2 is highly recommended), Windows 98, Windows 2000. Windows NT 4.0 (English language version) is recommended.
- The Microsoft TCP/IP protocol must be installed and configured.

Recommendations for Intel Device View for Web server:

- PC with a Pentium processor 200 MHz equivalent or faster, performance level or better, 64MB RAM, and an installed network adapter.
- A SVGA color display with a minimum resolution of 800 x 600 (1024 x 768 recommended) and 256 colors.
- Windows NT version 4.0 (server or workstation).
- The Microsoft TCP/IP§ protocol must be installed and configured.
- Web Servers: Microsoft Peer Web Services§ version 3.0 or later, Microsoft Internet Information Server§ (IIS) version 3.0 or later, Netscape Enterprise Web Server§ 3.51. These servers are automatically configured. Other servers may require manual configuration as documented in the readme.txt.

Recommendations for Intel Device View for Web client:

Intel Device View for Web clients use a Web browser to access Intel Device View for Web on a server. No software is required.

- PC with a Pentium processor 120 MHz equivalent or faster, performance level or better, 32MB RAM, and an installed network adapter.
- SVGA color display with a minimum resolution of 800 x 600 (1024 x 768 recommended) and 256 colors.
- Windows NT workstation or server version 4.0 (service pack 3 or higher recommended), Windows 95 (release A: service pack 1 or B: OEM 2 is highly recommended), Windows 98, or Windows 2000.
- Microsoft Internet Explorer§ version 4.0.

Requirements for Intel Device View as Plug-in

To run Intel Device View as a plug-in, the PC must be running HP OpenView§, Tivoli Netview§ or Intel LANDesk§ Manager.

To install Intel Device View

To install Intel Device View:

1 Insert the Intel Device View CD-ROM into the CD-ROM drive of your computer. The installation program starts automatically.

If the installation program does not start, do one of the following:

- Start Windows Explorer and right-click the drive containing the CD-ROM. Click **`Autoplay`** from the menu.
- Run `autoplay.exe` from the root directory of the CD-ROM.

2 Select the version of Intel Device View you want to install.

- Click **Install for Windows** to install Intel Device View on this PC.
- Click **Install for Web** to install Intel Device View onto a Web server.

  This provides access to Intel Device View from any client PC with a supported Web browser.
- Click **Install as Plug-in** to install Intel network device support for HP OpenView, Tivoli Netview, or Intel LANDesk Network Manager.

3 Follow the on-screen instructions.

After a successful installation, an Intel Device View program group appears in the Start menu of your desktop. See Chapter 3 “Managing the Router Using Intel Device View”, p. 37 to get further instructions on the use of Intel Device View.

Installing Adobe Acrobat Reader§ for Use with On-line Manuals

On-line manuals

The Intel Device View CD-ROM contains a number of Intel product manuals including a reference guide, user guides and quick start guides. The manuals are in PDF format and can be read using Acrobat Reader. If Acrobat Reader is not already installed on your PC, install it from the Intel Device View CD-ROM. The CD contains Acrobat Reader 4.0.

To install the Acrobat Reader

To install the Adobe Acrobat Reader version 4.0:

1 Insert the Intel Device View CD-ROM into the CD ROM drive of your PC.

2 From the Intel Device View installation screen, click **Install Add-ons**.

3 Select **Acrobat Reader 4.05** and click **Ok**. Follow the instructions on screen that follow.

Installing Internet Explorer

Internet Explorer for Intel Device View for Web

To use Intel Device View for Web from a client PC, the PC must be equipped with Microsoft Internet Explorer (version 4.0 or later). If your PC does not have a required version of Internet Explorer, you can install Internet Explorer version 5.0 from the Intel Device View CD-ROM.

To install Internet Explorer

To install Internet Explorer from the Intel Device View CD-ROM:

1 Insert the Intel Device View CD-ROM into the CD-ROM drive of your PC.

2 From the Intel Device View installation screen, click `Install` **Add-ons**.

3 Select **Internet Explorer v5.01** and click **Ok**. Follow the instructions on screen that follow.

Installing Shiva§ Configurator

Shiva Configurator

To manage Shiva network products from Intel Device View, you need to install the Shiva Configurator management software on your PC.

To install Shiva Configurator

To install Shiva Configurator from the Intel Device View CD-ROM:

1 Insert the Intel Device View CD-ROM into the CD-ROM drive of your PC.

2 From the Intel Device View installation screen, click **Install Add-ons**.

3 Select **Shiva Configurator v1.9** and click **Ok**. Follow the instructions on screen that follow.

3 Managing the Router Using Intel Device View

Intel Device View

Intel Device View is the recommended management software supplied with Intel network devices and can be used to configure and monitor most all router functionality. Intel Device View can be installed in the following versions.

Intel Device View for Windows

Intel Device View for Windows is a stand-alone program to manage Intel network devices that you install on one or more PCs on your network.

Intel Device View for Web

Intel Device View for Web is installed on a PC or Web server. You can access Intel Device View for Web from any PC on the network using a Web browser.

Install as a Plug-in

The plug-in versions of Intel Device View provide network support for HP OpenView, Tivoli NetView, and Intel LANDesk Manager.

Getting Started

To start Intel Device View for Windows

From your Windows desktop, click `Start` > `Programs` > `Intel Device View` > `Intel Device View - Windows`. The Intel Device View main screen appears.

To start Intel Device View for Web

To start the Web version of Intel Device View:

To run Intel Device View from the Web server

From your Windows desktop, click `Start` > `Programs` > `Intel Device View` > `Intel Device View - Web`. The Intel Device View main screen appears.

To view Intel Device View from a client PC on your network

Start Internet Explorer and enter the following URL in the address field:

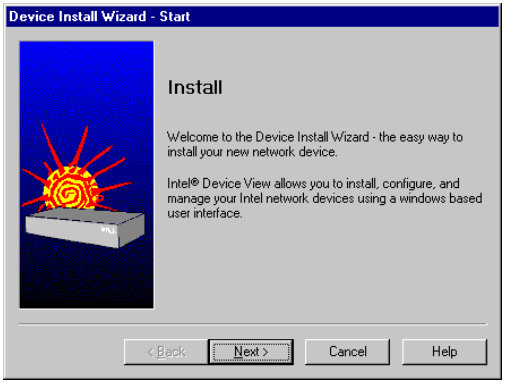
http://*servername*/deviceview/main.htm

where *servername* is the IP address or name of the Intel Device View server. The Intel Device View main screen appears.

To install the Express Router for management using the Install Wizard

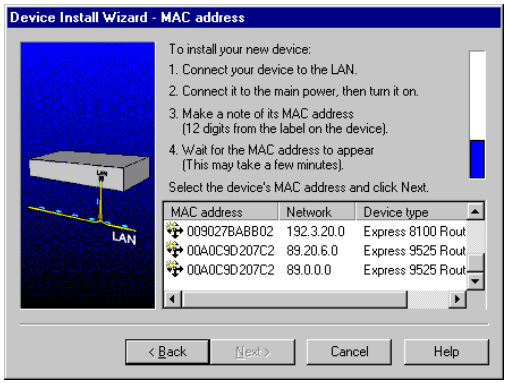
Use the Install Wizard to set up the router for management. The Install Wizard performs basic configuration such as assigning an IP address to the router.

1 From the Device menu, select Install.



Note Alternatively, you can select the MAC address from the Unconfigured Devices list of the Discovered Device Tree, and then follow the instructions.

2 Click `Next` and wait for the MAC address for your router to appear.



Note The Install Wizard can only be used for a router that has a factory default IP address indicated by the `Status` LED blinking green. If the router has already been assigned an IP address, click `Manage` from the `Device` menu. See “To manage a router” for details.

3 Click the MAC address and follow the on-screen instructions to complete the installation.

If the installation is successful, the router is displayed in Device View.

To manage a router

If a router has been assigned an IP address, open the router for management in Intel Device View by doing one of the following:

- Select Manage from the Device menu, then enter the IP address or DNS name for the router.
- Double-click on the icon for the router from the Discovered Device Tree of Intel Device View. For more information on the Discovered Device Tree, see “Using Device Tree”, p. 45.

On-line Help

On-line help features

Intel Device View has a number of on-line help features.

Help Topics

The Help Topics feature is a contents file to provide help on specific topics. To access the Help Topics, click `Help Topics` from the `Help` menu.

Context-Sensitive Help

Context-sensitive help provides information specific for a view or dialog box. To access context sensitive help:

- In the view or dialog press the F1 key.
- From the Help menu click `What's This` or from the toolbar and then click the dialog or view.
- From the dialog box click `Help`.

On-line Reference Manual

The on-line Reference Manual explains the functionality of the Express Router and associated networking concepts. The manual is available in PDF format on the Intel Device View CD-ROM in the Manuals directory.

To view the Reference Manual, insert the Intel Device View CD-ROM into the CD-ROM drive of your PC and click `Reference Manual` from the `Help` menu.

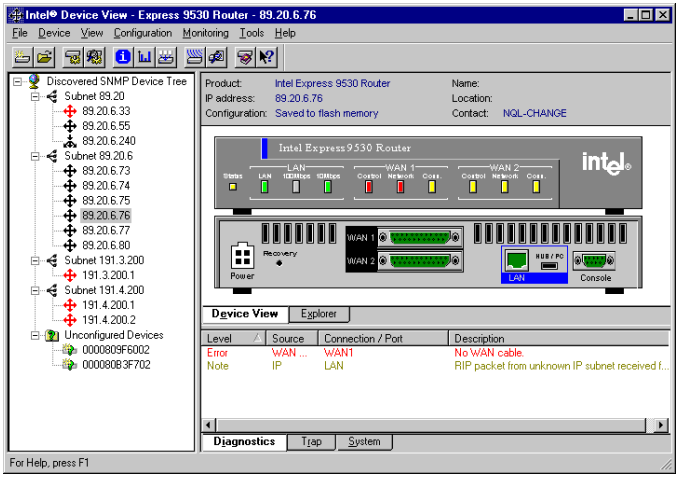
Note Acrobat Reader must be installed on your PC. See Chapter 2, “Installing Adobe Acrobat Reader§ for Use with On-line Manuals”, p. 34.

Intel Device View Display

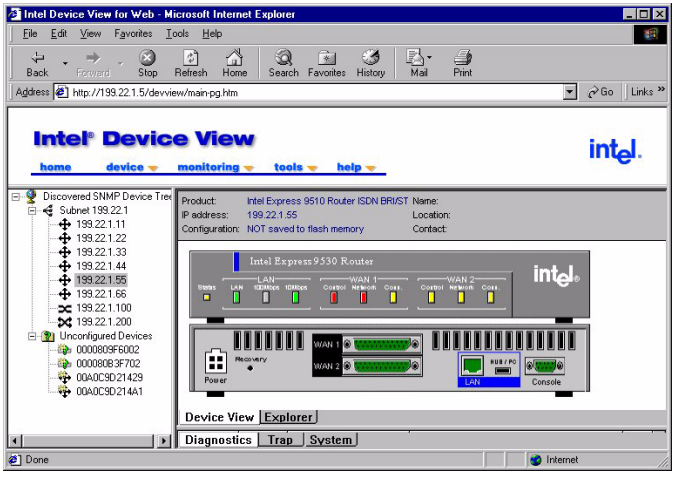
Main display

When a router is successfully contacted, the Intel Device View main display appears as shown in the examples.

Intel Device View for Windows



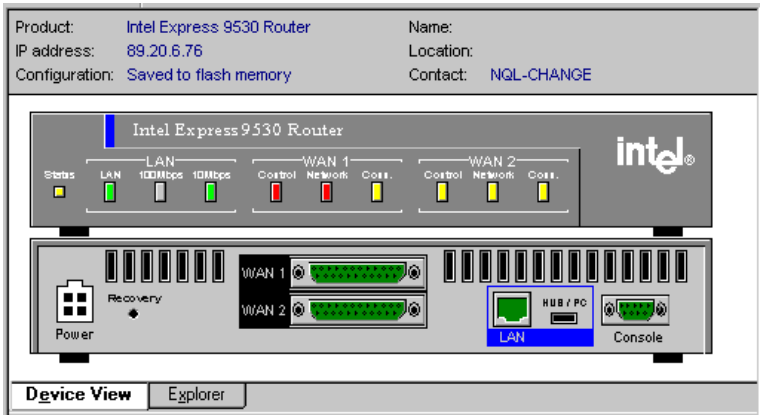
Intel Device View for Web



Device View

Device View

The Device View displays a real-time view of the front and back of the router and provides the state of LEDs and ports.



Main display color code

The router is displayed according to the following color code.

- Light gray body indicates the router is operational and can be managed by Intel Device View.
- Blue body indicates Intel Device View has lost contact with the router. This is caused by the router going down or being disconnected from the LAN.
- Dark blue body occurs when the you click the anywhere on the device.

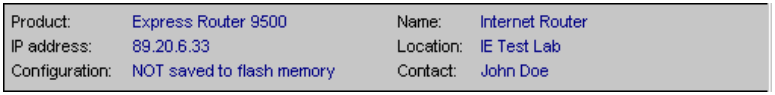
LEDs and ports on the main display

The LEDs represent the LEDs on the router itself and are updated every time Intel Device View polls the status of the router. If you position the mouse over an LED or port, a description of the LED or port and its state appears. The LED functions are described in Chapter 1 “LED Descriptions”, p. 5.

The polling interval determines how often the status is sampled and updated. To change the polling interval click `Preferences` from the `Monitor` menu.

Information panel

The Information Panel displays the product name, the assigned IP address, the status of the operational configuration, and the Name, Location and Contact person assigned to the router.



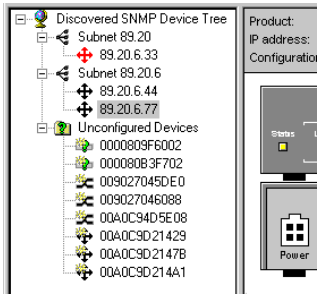
To enable or disable the Information Panel click `Information Panel` from the `View` menu or right click the device front panel and click `Information Panel`.

To edit the name, location, and contact person, click the System tab under `Configuration`>`Management Setup`.

Device Tree

Discovered Device Tree

Intel Device View automatically discovers supported Intel network devices. Discovered devices appear the Device Tree.



Configured devices are listed and grouped into separate folders. Click on (+) to expand a folder and (-) to collapse a folder. List devices by IP address or name and group by subnet, product, or device type (see “Device Tree right mouse click menu functions” in “Using Device Tree”, p. 46).

Device icons

Device Discovery uses the following icons to identify specific Intel network device types.

Icon	Device Description
Configured[1]	
	Router
	Switch
	Routing switch
	Hub
	Print server
Unconfigured	
	Unconfigured router
	Unconfigured switch
	Unconfigured routing switch
	Unconfigured hub
	Unconfigured print server
	Unconfigured device (unknown type)

[1] A configured device icon that is red indicates that Intel Device View has lost contact with the device.

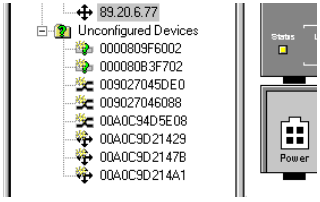
To set Device Discovery options

To configure Device Discovery options, such as discovery interval and polling interval, click `Device Discovery` from the `Device` menu.

Using Device Tree

Unconfigured devices

The Unconfigured Devices folder lists network devices that have a factory default configuration (no IP address) and devices in Recovery Mode. Devices are identified by their MAC address.



To configure a device, double click on the MAC address. A wizard guides you through initial configuration.

To add a device to the Device Tree

To add a configured device to the device tree:

1. Right-click anywhere on the Device Tree.
2. On the menu that appears click `Add Device`.
3. Enter the IP address for the device in the IP Address box. Enter the community read, community write and polling rate as required.
4. Click OK.

   An icon for the new device appears in the Device Tree.

To delete a device from the Device Tree

To delete a device from the Device Tree:

1. Right-click on the device you want to remove.
2. On the menu that appears click `Delete`.

   Note This does not affect the device. The device is still operational on the network.

To find a device in the Device Tree

To find a specific device in the device tree.

1. Right-click anywhere on the Device Tree.
2. Click `Find`.
3. Enter the IP address of the device.
4. Click OK.
   The device icon is selected in the Device Tree.

Device Tree right mouse click menu functions

Right click on the Device Tree to use these functions:

Function	Description
Launch With	This function is device specific. Gives access to the available launching tools for the device.
Group By	
Subnet	Group devices in folders by subnet number.
Product	Group devices in folders by product.
Device Type	Group devices in folders by device type.
Display By	
IP Address	Sort devices by their IP Address.
Name	Sort devices by name (if assigned).
Add Device	Add a device to the tree.
Delete	Remove the selected device from the device tree. This does not affect the actual device.
Edit	Edit information for the device stored in the Device Discovery database, such as minimum polling rate.
Find	Locate a specific device in the tree by searching for its IP address.
Refresh	Poll the network and updates the devices in the tree. If a new device has been connected to the network, it should appear after refresh.

Note Menu items can vary between devices.

Additional Functions

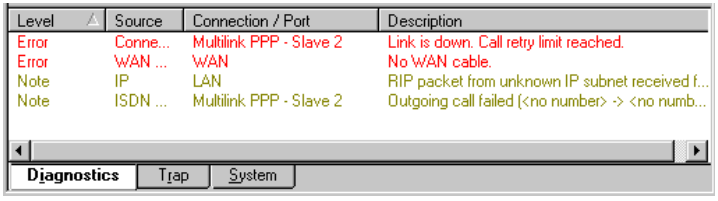
Use the Device Tree to perform these functions:

- To manage a configured device, double click the device icon.
- To start the Install Wizard, double-click on the unconfigured icon.
- To display product information such as product name and version number, click the icon.
- To display the user-defined device name, position the mouse over the device.

Diagnostics Window

Diagnostics window

The Diagnostics window allows you to troubleshoot the router in case of problems.



The Diagnostics window displays problems currently detected by the router.

- The entries are color coded according to the level of severity.
- Entries are displayed in order of occurrence and can be sorted according to fields.
- The diagnostic entries are removed from the list when the router detects the problem no longer exists.
- Diagnostic messages are recorded in the System Log.

Diagnostic fields

Each diagnostic message includes these fields.

Field	Description
Level	Indicates the severity of the message.
Source	The protocol or feature affected by the error, for example, ISDN, firewall, PPP.
Connection/Port	The name assigned to the connection and port on which the problem occurred.
Description	A brief explanation of the problem.

Diagnostic levels and color coding

Diagnostic messages are color-coded according to three levels of severity.

Level	Color	Interpretation
Fatal Error	Red	Serious errors in the router. Try to restart the router. If the problem persists, double-click on the diagnostic message to display a description of the problem. The Status LED on the router is steady red.
Error	Red	Operational errors often caused by configurational mismatches, cables, network problems, and so on. The router is operational but a particular function may not. Display the corrective action for these errors (see below) and follow the instructions to correct the problem. Status LED on the router is steady red.
Note	Dark yellow	Note messages are not errors but may require attention. The router is fully operational. These messages relate to the performance of the router. For example, a connection runs with the data compression disabled due to a mismatch in configuration between this router and the router over the WAN.

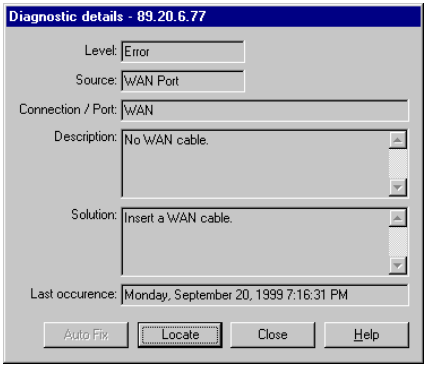
To enable or disable color coding

To enable or disable color coding of messages, right-click the Diagnostic Window and click `Use Color Coding`.

Using Diagnostics

To display corrective action

To display a description of the problem and suggested corrective actions, double-click on the diagnostic message or right-click and click `Details`.



To display monitoring information (counters and statistics), click Locate.

To correct problems using Auto Fix

To automatically fix a problem click `Auto Fix`. Not all diagnostics are supported by autofix. Typical problems include:

- Call Retry Limit exceeded for a connection.
- Daily Activity Limit for the use of a connection has been exceeded.
- Wrong IP RIP version of the router for the LAN or a WAN connection.

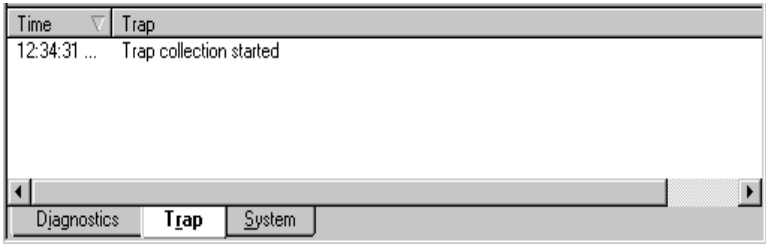
To sort diagnostic messages

To sort the diagnostic messages on any of the fields, click the field heading.

Trap Window

Trap window

The Trap window displays all SNMP traps generated by the router. Traps can be normal operating events (such as WAN connections going up or down) or they can be errors (such as device failure) in the router.



Trap window that runs on Intel Device View for Web displays the SNMP traps from all devices on the network.

Note Intel Device View for Windows will only receive traps from a device if the PC is configured as a trap destination in the device. This is done automatically when the router is initially installed using the Intel Device View Install Wizard. See “Management setup in Intel Device View”, p. 72.

Trap severity and color coding

The SNMP traps are color-coded according to their level of severity as follows (listed in order of increasing severity):

- Level 1 Traps - black
- Level 2 Traps - dark gray
- Level 3 Traps - dark yellow
- Level 4 Traps - orange
- Level 5 Traps - red

Using Trap Window Options

Color coding traps

To enable or disable color codes for traps:

1. Right-click in the Trap window.
2. Click Properties.
3. Select the color code option.

To set a maximum number of traps

To set the maximum number of traps that can be stored in the Trap window:

1. Right-click the Trap window.
2. Select Properties from the menu.
3. Enter a number in the Max. messages to store field.

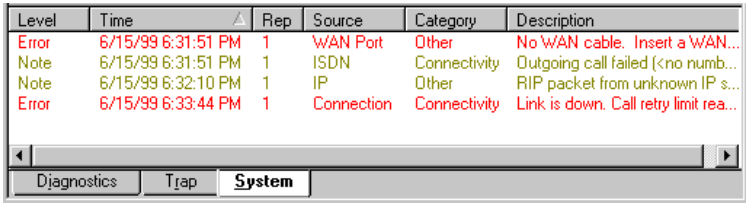
To clear traps

To clear all traps from the Trap window, right-click the Trap window and select `Clear`.

System Window

System window

The System window displays the System Log from the router.



The System Log contains a history of events in the router.

Note Use Advanced Setup to configure messages displayed in the log. See “Configuring the Log System”, p. 253.

System window fields

System window messages include these fields:

Field	Description
Level	Indicates the level of severity of the message.
Time	Indicates the date and time of the event.
Rep	Shows the number of times the event has occurs in the log.
Source	The protocol or feature affected by the error, for example, ISDN or PPP.
Category	A high-level classification of the message, such as security, accounting or connectivity.
Description	A brief description of the event.

System message levels and color coding

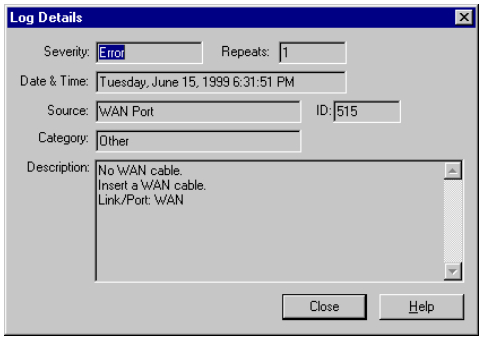
System window message levels in order of decreasing severity:

Level	Color	Interpretation
Fatal error	red	Serious errors in the router. The router is non-operational.
Error	red	Operational errors caused by configurational mismatches, cables, network problems, and so on.
Note	dark yellow	Significant information about the performance or fine-tuning of the router.
Info	green	General information not significant to the operation, such as accounting information.
Debug	black	Very low level informational message.

Using the System Window Functions

To view message details

To obtain details about a message double-click on the message or right-click the message and click `Details`.



To save a system log

To save a system log to a specified destination as a CSV file:

1. Right-click the System window.
2. Click `Save`.
3. Enter the destination and name of the file.
4. Click `Save`.

To clear the system log

To clear the system log right-click the System window, then select `Clear`.

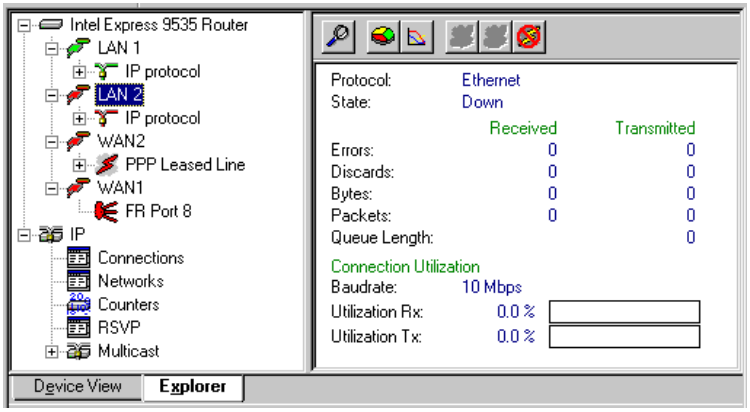
To filter messages from display

You can filter messages from the display based on level, source, or category. See Chapter 11 “Configuring the Messages Included in the Log System”, p. 255.

Explorer View

Explorer View

The Explorer View allows you fully manage the router from a tree structure.



The left window displays the ports, connections, and protocols configured on the router. The right window displays information about the selected item on the left. Ports, connections, and protocols are color coded to indicate the current state.

Color codes for ports, connections and protocols

The Explorer uses these color codes:

Color	Description
Green	The port, connection or protocol is operational (up).
Red	The port, connection, or protocol is not operational (down).
Yellow	Connection is in timecut. This is used for switched on-demand (dial-up) connections such as ISDN or X.25.
Blue	Intel Device View has lost contact to the router.

Organization of the Explorer Tree

The Explorer information is organized in layers from the WAN ports, to the network protocols, and to the protocols that run on top of the network protocols, such as IP RIP, IPX RIP and SAP, Bridging BPDU.

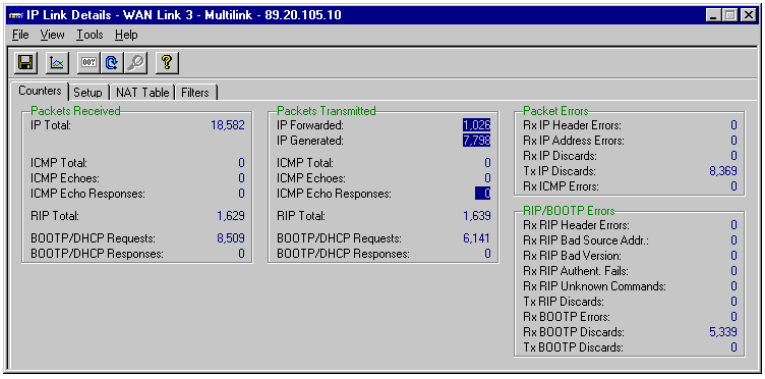
The Explorer works in the same way as Windows Explorer. Click (+) to expand layers and (-) to collapse. Click on the layer to display data.

Explorer functions and additional information

The Explorer offers a number of additional functions accessed from the toolbar or by right-clicking the mouse.

Details

Extensive monitoring details of all the protocol and facilities supported by the router are available by selecting the connection or protocol of interest in the Explorer window and click on the Details button.

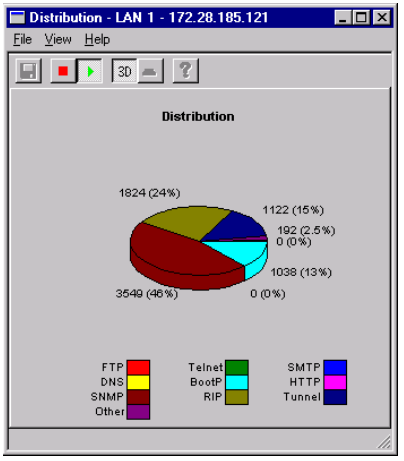


Information is arranged in tabbed dialogs where appropriate.

To get management parameter descriptions, click or F1.

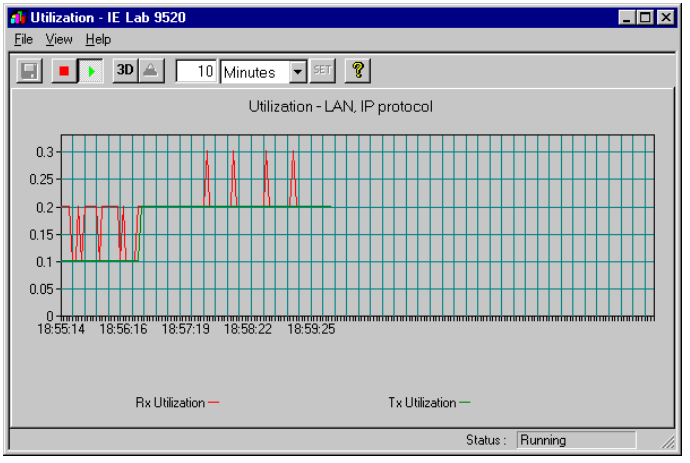
Distribution

Display distribution of the data traffic of each protocol available on the connection.



Utilization

Plot a graph of the utilization of a connection over time.



Force Up Connection

Force the selected connection into the up state, for example, if the connection was in time-cut.

Force Down Connection

Force the selected connection into the down state. The connection is brought up the next time a packet need to be routed on the connection.

Disable/Enable Connection

Disable or enable the selected connection.

Configuring the Router Using Intel Device View

Connection Setup and configuration programs

Connection Setup is a wizard based program to configure the ports and connections on the router. The configuration meets the requirements for most installations without further configuration. In addition, these programs are available from the `Configuration` menu.

- **Management Setup** configures the general system information and management access rights.
- **IP DHCP Setup** configures the DHCP server in the router.
- **IP NAT Table Setup** configures NAT entries.
- **IP Static Routes** configures IP static routes on WAN and LAN connections.
- **IP Filter Setup** defines firewall and IP filtering on LAN and WAN connections.
- **Advanced Setup** is a menu-based configuration tool providing full configuration suited to the more advanced user.

Use Connection Setup to configure the router initially, then use the other configuration programs to customize and fine-tune the configuration as necessary.

Note If you use Connection Setup on a port or connection that has been configured using a configuration program other than Connection Setup, such as Advanced Setup or IP Setup, some configuration parameters may be overwritten or lost.

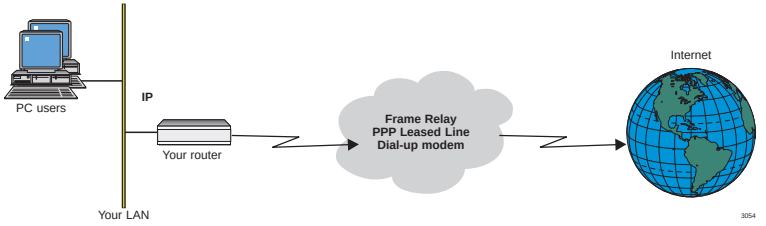
Configuring Ports and Connections Using Connection Setup

Connection scenarios offered by the Connection Setup

Connection Setup provides the following scenarios for setting up connections on your router. Choose the scenario which best matches the use of your router.

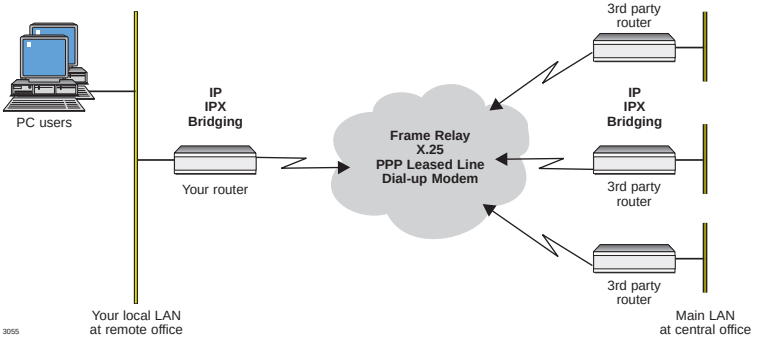
Internet Access via an Internet Service Provider (ISP)

Connect your Local Area Network (LAN) to the public Internet via an Internet service provider (ISP). Connections to the Internet are supported via leased lines, Frame Relay, and a PPP dial-up modem on the console port.



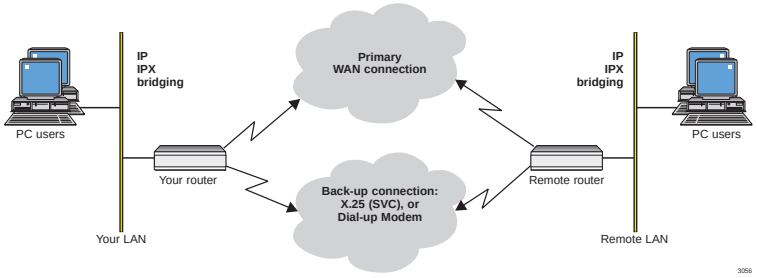
Direct connection to a remote site

Connect your Local Area Network directly to a remote site. Connections to remote sites are supported via leased lines, Frame Relay, X.25 (PVCs and SVCs), and a PPP dial-up modem on the console port.



Backup Connection

Establish a backup connection in the event the primary connection fails. Backup connections must be dial-up connections such as X.25 SVCs or a PPP dial-up modem on the console port.



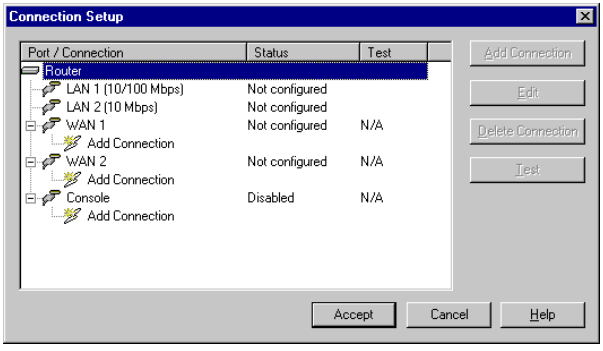
Information required for Connection Setup

Obtain most of the information for configuring ports and connections from your service provider or subscription. Use the configuration work sheets supplied with the Quick Start to help gather the information.

Accessing Connection Setup

To access Connection Setup

Click Connection Setup from the Configuration menu, or click from the toolbar.



This screen displays the available router ports and the remote connections configured on each port. Click (+) to expand the tree and (-) to collapse it.

From this screen configure the ports and add, edit, and delete remote connections.

Note The test column is static, indicating the result from the last test performed. To obtain a current status use the `Test` button or use the Explorer view.

Firmware upgrade detection

When you access Connection Setup, Intel Device View compares the firmware installed in the router to the firmware installed in Intel Device View. If Intel Device View includes a newer version of firmware, you are asked to download the upgrade.

If you choose to upgrade, the Firmware Upgrade Wizard starts the installation. See “Upgrading and Managing the Router Firmware and Plug-ins”, p. 73.

Note If you choose not to upgrade, you can run the upgrade wizard later. From the Device menu, click `Firmware`.

Configuring a WAN Port (WAN, CSU/DSU, HDSL2, and Console port)

To set up a port

Before a connection is set up, configure the port according to the service subscription. To set up the port:

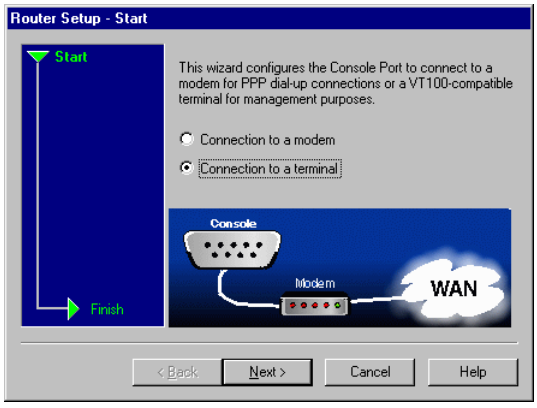
1 From within Connection Setup, do one of the following.
- double-click the port icon.
- click the port and then click Set Up Port.

2 The port setup wizard guides you through configuration.

To set the console port to terminal mode

Use Connection Setup on the console port setup to console port to connect to a VT100-compatible terminal.

1 Click the console port and click `Set Up Port`.



2 Select the `Connection to a terminal` check box and click `Next`.

The console port is in terminal mode. PPP dial-up connections via the console port are disabled.

To test the port

To test the cable connection on the port, select the port then click the `Test` button. This test will also autodetect the CSU/DSU parameters for T1 connections on the CSU/DSU port.

Adding and Editing Remote Connections

To add a remote connection

After the port is configured, you can add remote connections.

1 From the Connection Setup screen, do one of the following.

- double-click the `Add Connection` icon under the port, and select the scenario from dialog box that appears.
- double-click on the connection type icon under the port.
- click the port and then click `Add Connection`.

2 The connection setup wizard guides you through configuration.

To test a connection

To test if a connection is operational, click the connection and then click Test.

To delete a connection

To delete a connection, click the connection and then click `Delete Connection`.

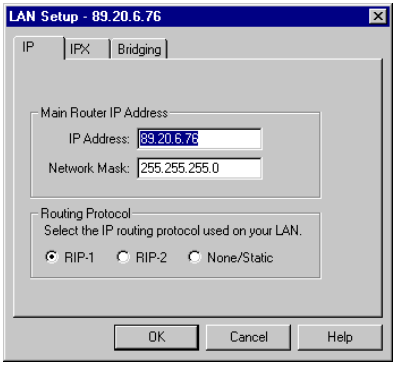
Configuring LAN Ports

LAN port configuration

Use the LAN port setup in Connection Setup to configure the required routing protocols for your LAN (IP, RIP, IPX, and Bridging). It is through the LAN port configuration that you can set the IP address of the router LAN.

To set up LAN ports

From the Connection Setup screen, double-click the LAN port icon or click the port then click `Set Up Port`.



Click on the tabs and configure the routing protocols as required. Use on-line help for guidance and descriptions of screen parameters.

LAN port default settings

The default routing on the LAN port is:

- IP Routing with RIP-1 is enabled
- IPX Routing is disabled
- Bridging is disabled.

Exiting Connection Setup

To exit Connection Setup

To exit Connection Setup:

- Click Accept to keep the changes.

  The changes are not permanently saved in the router. To save the changes permanently, click Save to flash from the Configuration menu.

- Click Cancel to discard the changes.

Configuring the DHCP Server

DHCP server

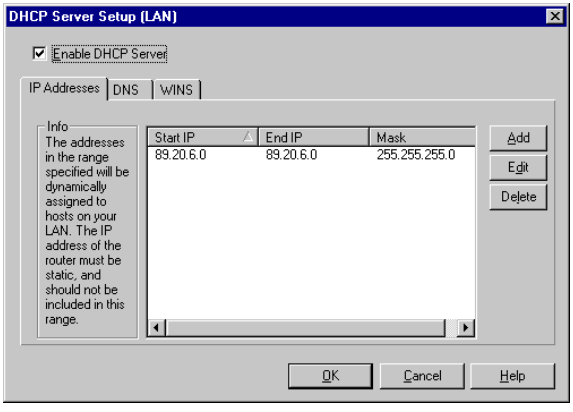
Use the DHCP (Dynamic Host Control Protocol) server in the router to dynamically assign an IP address and other information to network devices (clients). The DHCP server can:

- assign an IP address, subnetmask, and default gateway address.
- assign a DNS (Domain Name System) server.
- assign WINS (Windows Internet Name Service) server.

See the Reference Manual for detailed explanation of how DHCP server works.

To access the DHCP server setup

To access the DHCP server setup click `DHCP Server` from the `Configuration` menu.



The dialog displays the IP address ranges configured for use in the DHCP server.

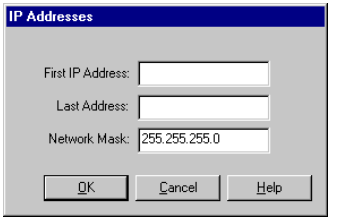
To enable or disable the DHCP server

From the DHCP Server Setup screen, select or clear the `Enable DHCP Server` check box.

To add or edit IP addresses in the DHCP server

To add, edit or delete an IP range in the DHCP server:

1. From the `DHCP Server Setup` screen:
   - Click `Add` to add a new range of IP addresses.
   - Select the IP address range you want to edit and click `Edit`.
   - Select the IP address range you want to delete and click `Delete`. Go to step 3.
2. Enter the IP addresses and network mask for the range.

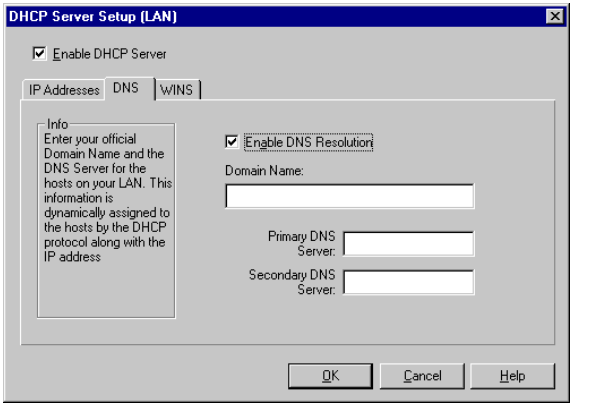


3. Click `OK` to accept changes or Cancel to discard changes.

To configure a DNS server in the DHCP server

To configure the DHCP to assign a DNS server to devices requesting an IP address:

1. From the `DHCP Server Setup` screen, click the `DNS` tab.



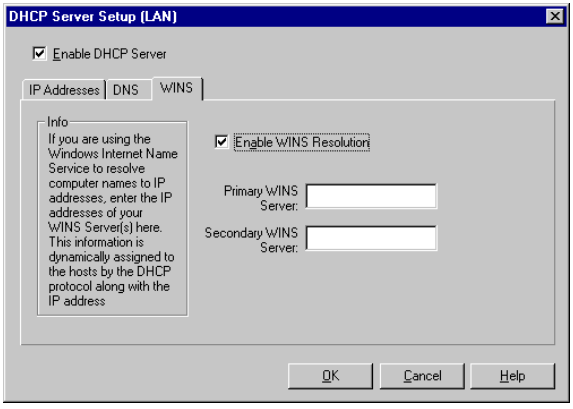
2 To enable this feature, select the `Enable DNS Resolution` check box. If you clear this box, DNS information is not assigned to devices that request an IP address.

3 Enter the DNS server parameters and click `OK` when completed.

To configure a WINS server in the DHCP server

To configure the DHCP to assign a WINS server to devices requesting an IP address:

1 From the `DHCP Server Setup` screen, click the `WINS` tab.



2 To enable this feature, select the `Enable WINS Resolution` check box. If you clear this box, WINS information is not assigned to devices that request an IP address.

3 Enter the WINS server parameters and click `OK` when completed.

Configuring IP Network Address Translations

IP Network Address Translation

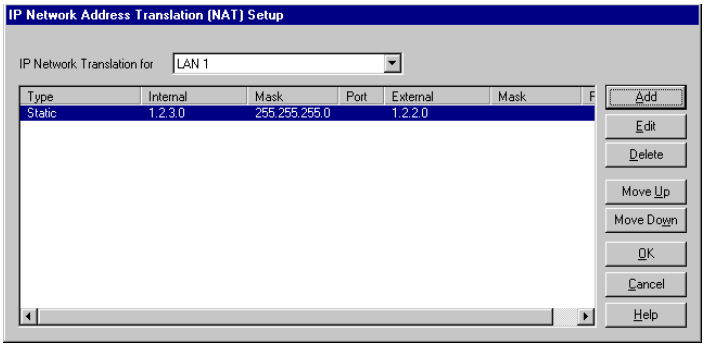
Network Address Translation (NAT) translates local (private) IP addresses to remote (public) IP addresses. This is typically used when you are connecting to the Internet via an Internet service provider (ISP). The ISP assigns one or more IP addresses for use from your site. If you use private IP addresses on your LAN, NAT translates these addresses to the ISP assigned addresses.

For additional information about IP NAT, refer to “Network Address Translation (NAT)”, p. 192.

To set up IP NAT

To set up the IP NAT table for the Express Router:

1 From the `Configuration` menu, click `IP Setup`> `NAT Table`.



The current NAT entries appear for a selected connection.

Note The order of the entries is important. The router will translate addresses according to the first matching entry in the table. Other relevant entries are ignored. See “Network Address Translation (NAT)”, p. 192 and the Reference Manual for details.

2 From the `IP Network Translation` drop down list, select the connection.

3 To add or edit entries:

- To add a NAT entry, click `Add` and configure the parameters.
- To edit an existing entry, click the entry and click `Edit`. Configure the parameters.
- To delete an entry, click the entry and then click `Delete`.
- To move the position of an entry, click `Move Up or Move Down`.

Use the on-line help for explanations of screen parameters.

4 To save the settings click `OK`. To discard the settings, click `Cancel`.

Configuring IP Static Routes

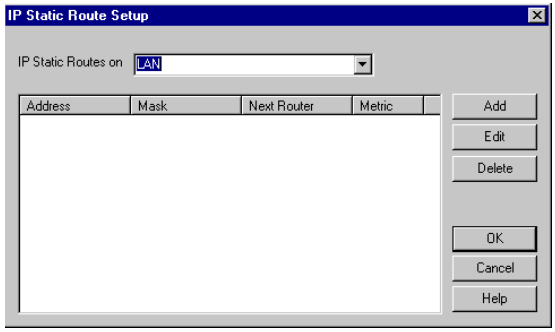
IP static routes

IP static routes are routes that are manually configured in the router. You should establish static routes if you want to route data to a few destinations without using the Routing Information Protocol (RIP). RIP updates take up bandwidth over WAN connections, thus establishing a static route can free up some bandwidth.

To configure IP static routes

To add or edit static routes to the Express Router:

1 From the `Configuration` menu, click `IP Setup`>`Static Route`.



The current static routes appear for a selected connection.

2 Click the connection from the `IP Static Routes on` drop down list.

3 To add or edit specific routes:

- To add a new static route, click `Add` and configure the route parameters.
- To edit an exiting static route, click the route and click `Edit` then configure the route parameters.
- To delete a route, click the route and then click `Delete`.

4 To save the settings click `OK`. To discard click `Cancel`.

Configuring IP Filters and Firewalls

IP filtering

IP filters restrict access between networks and network devices and reduce unnecessary data traffic. Use IP filters to build your firewall. Filters are configured on a connection basis. You can configure transmit (data leaving the router) filters and receive (data entering the router) filters for static and stateful pass filters.

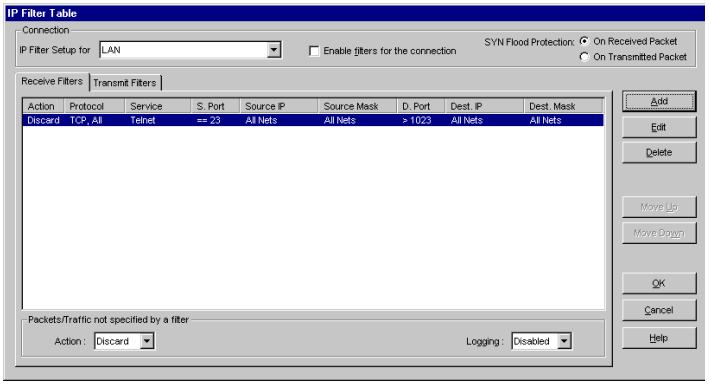
- Static filters are available for all IP protocols. They can either pass or discard traffic that meets the filter criteria you define.
- Stateful pass filters are a type of dynamic filter available for TCP, UDP and ICMP protocols. Stateful pass filters remember source and destination addresses and port numbers of outgoing traffic. It virtually opens a hole through the firewall to allow traffic to pass. Only incoming traffic that matches the outgoing traffic information is allowed back in through the firewall. The filter is also time-limited. If a valid response is not received within a certain period of time, traffic is not allowed to pass by the filter. These characteristics make stateful pass filters more secure than static filters.

For more details on static and stateful pass filters, see “IP Filters and Firewall Protection”, p. 167.

To set up IP filters

To add or edit IP filters.

1 Click `IP Setup`>`Filters` from the `Configuration` menu



The IP Filter table shows the current IP transmit and receive filters for a selected connection.

The order of the filters is important. The router filters IP packets on the connection using the first matching filter in the table, working from top to bottom. Other relevant filters are ignored. See “Packet processing by filters and filter order”, p. 169 for an explanation of this process.

2 Click the connection from the `IP Filter Setup for` drop down list.

3 Click the `Receive Filters` or `Transmit Filters` tab, depending on the type of filter.

- Receive filters prevent unauthorized access to the router.
- Transmit filters limit data traffic out of the router.

4 To add or edit specific filters:

- To add a new filter, click `Add` and configure the filter parameters. Use online help for a detailed explanation of parameters and settings.
- To edit an exiting filter, click the filter and click `Edit`. Configure the filters. Use online help for a detailed explanation of parameters and settings.
- To delete a filter, click the filter and click `Delete`.
- To move the position of a filter, click `Move Up or Move Down`.

5 Set the Action for packets/traffic not specified by a filter to `Discard` or `Pass`.

- Discard blocks the IP packets unless they are allowed to pass by a specific filter. This is a static filter.
- Pass transmits IP packets unless they are discarded by a specific filter. This is a static filter.

6 Select traffic on which you want to apply the SYN Flood protection. The default is On Receive Packet and is suitable for most installations. For more details, see the on-line help or “SYN Flood Protection”, p. 172.

7 Select the Enable filters for the connection check box.

8 Select `OK` to save the settings or `Cancel` to discard them.

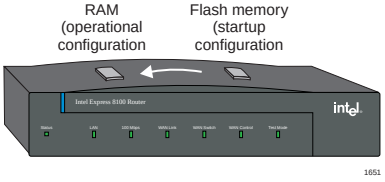
Configuration Management

Configuration management options

The Configuration menu of Intel Device View offers these options for managing the router configuration:

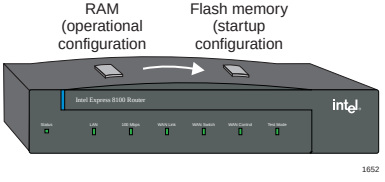
Restore from Flash Memory

Reloads the permanent configuration for the router from flash memory, overwriting the current configuration. Any configuration changes made since the configuration was last saved to flash memory will be lost.



Save to Flash Memory

Saves the current active configuration to flash memory as the permanent configuration. The new configuration is used when the router is restarted. The existing configuration in flash memory is lost.



After the router configuration is changed, the new configuration is stored temporarily in RAM and is immediately operational. To keep the new configuration, you must save it to flash memory as the permanent configuration.

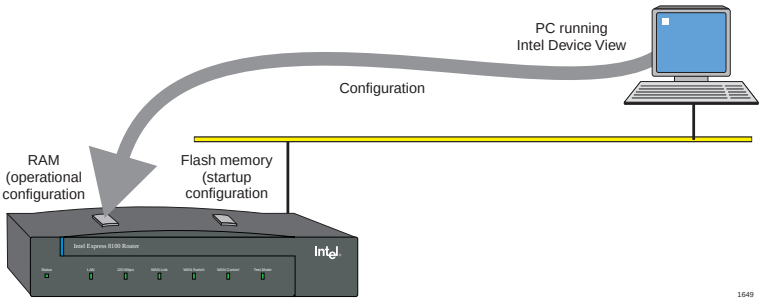
If the router is rebooted or reset before the new configuration is saved, the new configuration will be lost.

Restore from Disk

Restores a router configuration previously backed up to the hard drive.

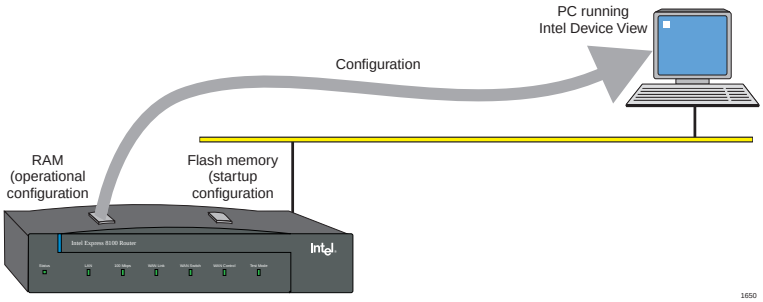
If the current router configuration has not been saved, it is overwritten and lost.

The restored configuration must be saved to flash memory to use it as a permanent configuration.



Backup to Disk

Saves the current active configuration to the hard drive as a backup.

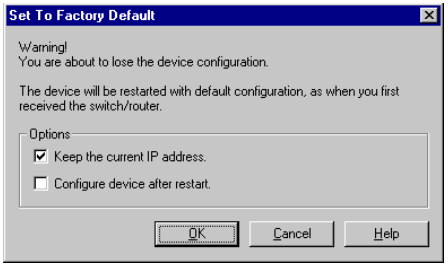


You can save a number of backup files, identifying each by a unique file name.

Note The current active router configuration is backed up which may be different from the permanent configuration stored in flash memory.

Restore Factory Default

Resets your Express Router to the factory default configuration. See “Router Factory Default Setup”, p. 21. The current router configuration is lost.



You can reset the IP address to factory default or keep the current IP address. If you reset the IP address to the factory default, you must use Install to reinstall the router. If you keep the current IP address, use Manage to access the router.

Reboot

To restart the router, click the `Reboot` from the Device menu. If the configuration for the router has changed and is not saved to flash memory as the permanent configuration, you will be asked if you want to save the new configuration before reboot.

Management setup in Intel Device View

To change these parameters from Intel Device View, select `Management Setup` from the `Configuration` menu.

System Details

Assign a name, location and a contact person to the router.

Date and Time

Set the internal clock of the router.

Authentications

Define which network management stations have access to the router for management and configuration purposes according to protocol (SNMP, TFTP, Telnet).

Traps

Set or edit SNMP Trap destinations. SNMP Traps alert you of any changes that occur in the router.

Local Management

Set or edit passwords to access Local Management on the router from a Telnet session or from the console port. You can also define a timeout period o automatically close a Telnet session.

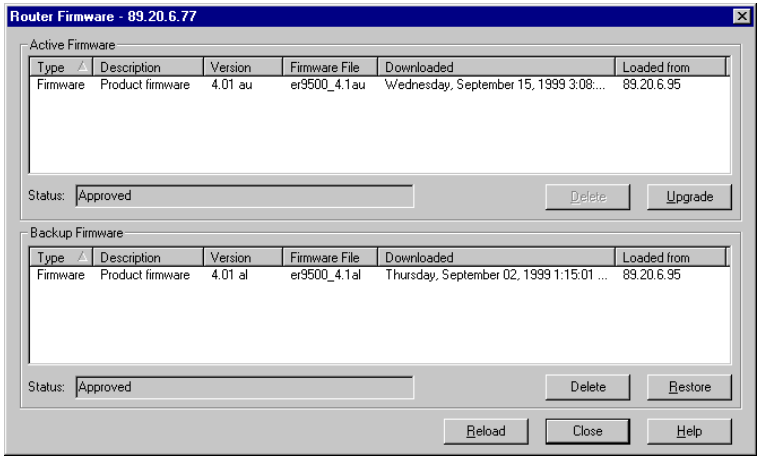
TFTP

Set or edit a TFTP access password. TFTP is used to configure the router and to update the firmware.

Upgrading and Managing the Router Firmware and Plug-ins

Firmware and plug-in management

To access the router firmware and plug-in management options, click `Firmware` from the `Device` menu.



The screen provides information on the current firmware and plug-ins.

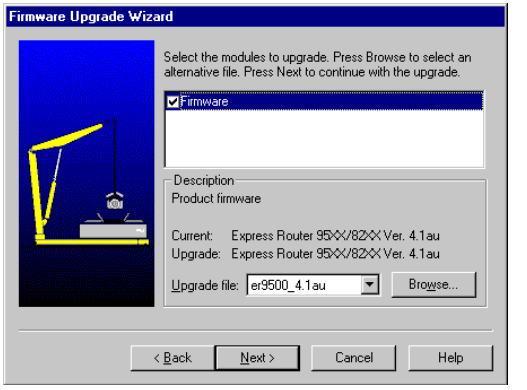
From this screen, you can download new firmware or plug-ins using the Firmware Upgrade Wizard, or restore backup firmware and plug-ins.

To upgrade the firmware or plug-in

To upgrade the firmware or plug-ins:

1 Click `Firmware` from the `Device` menu.

2 From the `Router Firmware screen`, click `Upgrade`>`Next`.



3 To complete the upgrade, follow the on-screen instructions.

The previous active firmware or plug-in module becomes the backup.

Safe firmware upgrade

To ensure safe upgrade, the router checks the new firmware after download. If the router detects an error or cannot contact Intel Device View, the router automatically reverts to the old firmware.

To restore backup firmware and plug-in modules to the router

To restore a backup firmware or plug-in module:

Note The Restore feature restores all backup firmware and plug-in modules. Single selection is not possible.

1 Click `Firmware` from the `Device` menu.

2 From the `Router Firmware` screen, click `Restore`.

Follow the on-screen instructions.

Managing Licensed Software

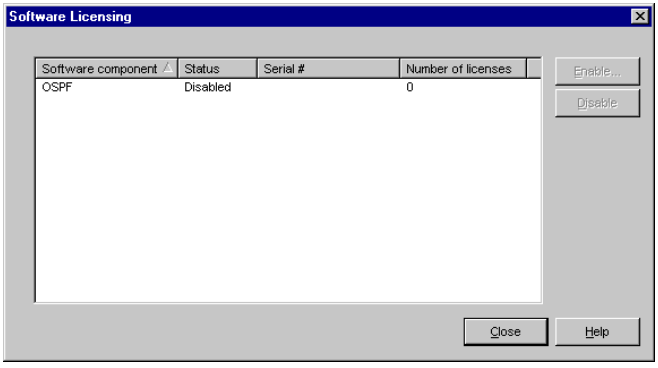
Licensed Software

The router supports a number of software features, such as OSPF, that you can purchase to upgrade the functionality of the router. You can purchase single or multiple device licenses. Upon purchase, you receive a license key that you must enter to activate the feature. The software licensing feature allows you to control the use of your licenses.

To enable or disable a Software License

To enable or disable a software license:

1 Click Software Licensing from the Device menu.



2 Select the software component and then click Enable to activate the license or Disable to remove the license.

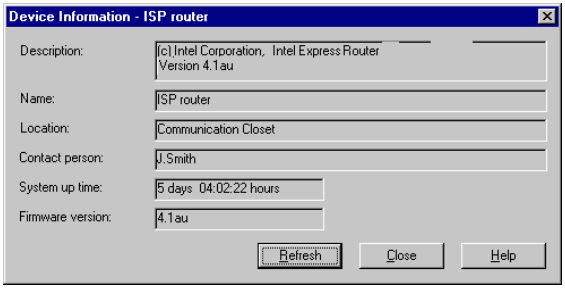
If you choose to enable a license, you will be prompted to enter your license-key for the feature. Enter the license key as it appears on your software license agreement.

Monitoring the Router

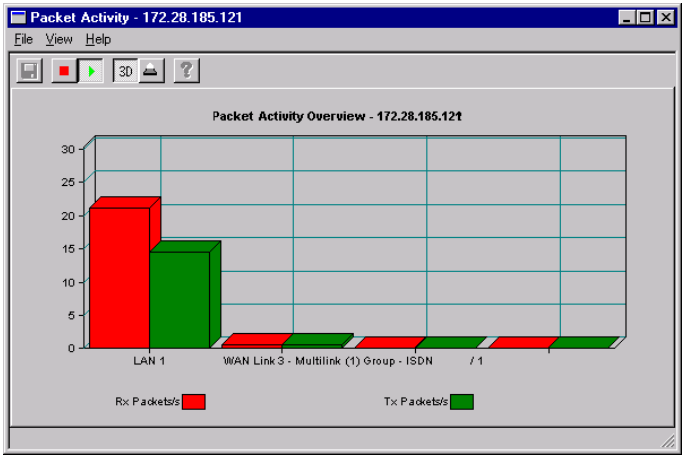
Monitoring information available

Intel Device View provides monitoring capability available from the `Monitoring` menu. The following is an overview of the monitor features. Use the on-line help to obtain information about monitor screens and their contents.

View Device and Hardware information

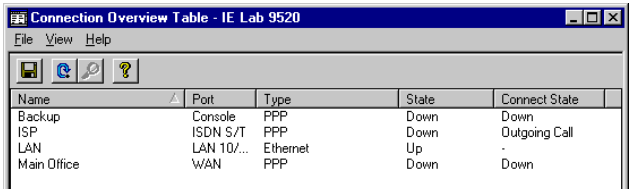


Monitor Connection Activity

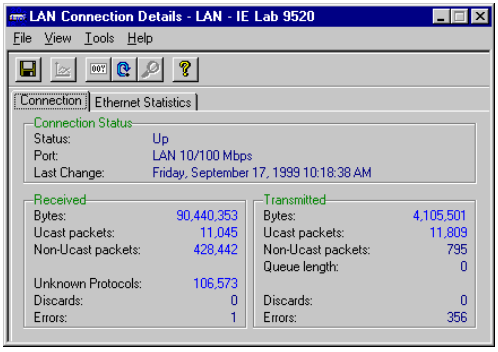


View packet activity (transmitted and received), errors and discards, and utilization of the connection.

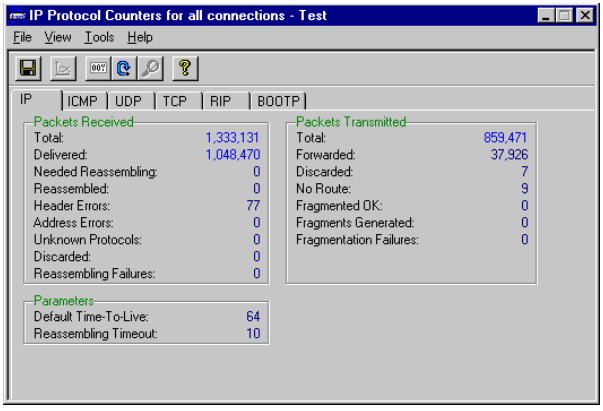
Overview of the router connections



To access details for connections, double-click the connection or click the connection and then the click .



Routing protocol and bridging information for the router.



This information includes:

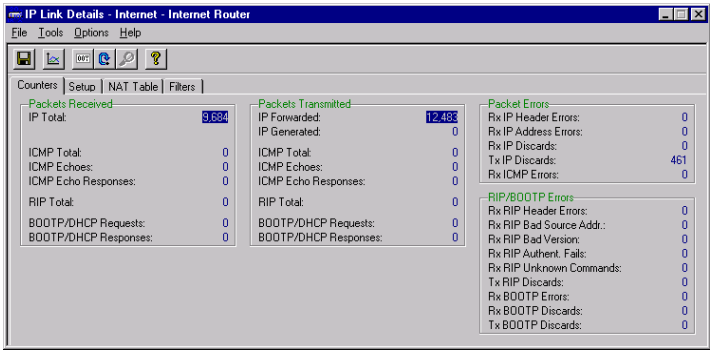
- overviews of the router connections on which the routing protocol or bridging is configured.
- networks and services tables.
- protocol counters and statistic.

Plotting Management Information

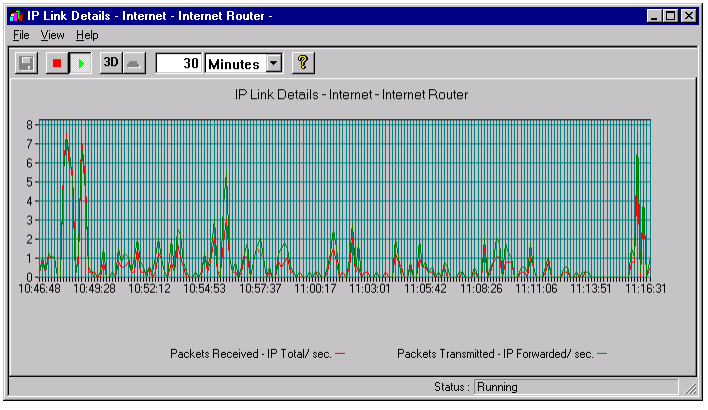
To plot a graph of counters

To plot counters from the counters or statistics screens:

1 Click the counters to be plotted. Selected counters are highlighted.



2 Click `Graphs` from the `Tools` menu or click .



Use the tool bar or View menu to change the display.

Setting Monitor Preferences

Monitor preferences

To define how Intel Device View monitors a router, click `Preferences` from the `Monitoring` menu.

Preference	Use
Polling	Set polling time interval for sampling the router configuration and status.
Monitor	Set update time interval for graphs and windows displaying router statistics.
Timeout	Set polling timeout parameters for SNMP.
Community	Assigns the community that SNMP uses when polling a devices.

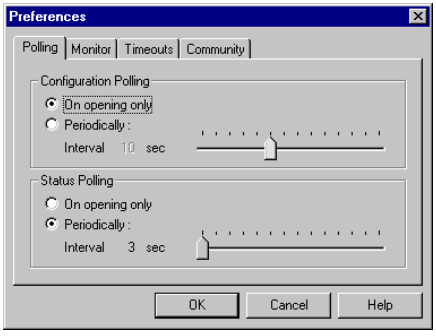
The settings apply only to the router or device currently open in Intel Device View.

Note Short polling intervals can increase the amount of traffic on the network. See “Setting the Polling Parameters”.

Setting the Polling Parameters

To set the polling intervals

The polling intervals determine how often Intel Device View polls the router and updates the status, such as the state of the LEDs. To access the polling parameters, click `Preferences` from the `Monitoring` menu.



Setting the polling parameters for slow connections

Monitoring information from the router is obtained using SNMP. SNMP increases network traffic which may be an issue when managing the router over a slow WAN connection. To reduce network traffic caused by SNMP, increase the polling interval and the timeout value for replies.

4 Introduction to Local Management

Local Management

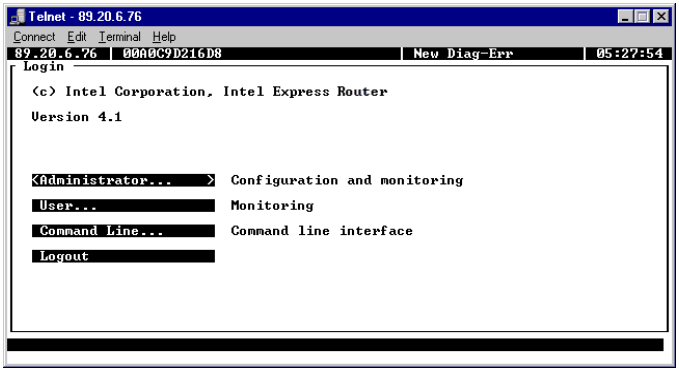
Local Management is a menu-based management and configuration tool that runs on-board the router.You can access Local Management from any telnet session to the router or from a VT100-compatible terminal connected to the console port.

Intel Device View is the recommended management tool. Use Local Management to configure and monitor the router as an alternative to Intel Device View.

Local Management Access Using Telnet

Starting a Telnet session to a router having an assigned IP address

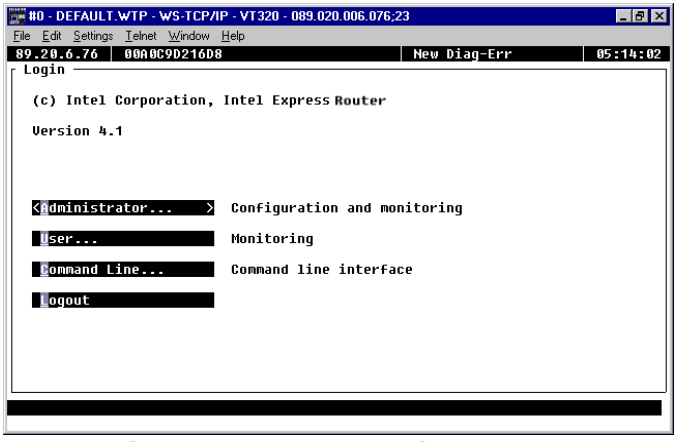
If the router has been assigned an IP address, you can access Local Management by establishing a Telnet session on the IP address of the router. When the session is established, the Login screen appears:



To access Local Management from Intel Device View using Telnet

If the router has been assigned an IP address, you can access Local Management within Intel Device View by doing one of the following:

- Manage the router and select `Telnet` from the `Tools` menu.
- From the `Tools` menu click `Telnet` and type the IP address of the router.



Log in to Local Management. See “Local Management Login”, p. 88

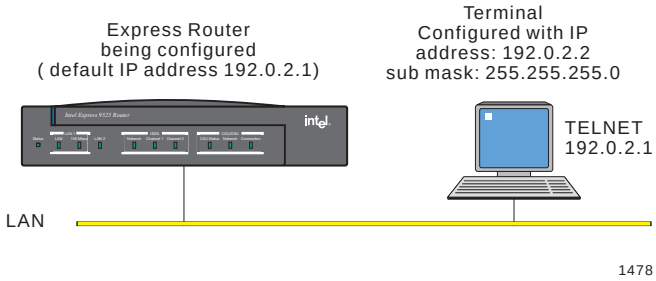
To start a Telnet session to a router having a default IP address

The Express Router is assigned a factory default IP address of 192.0.2.1 for LAN and LAN1 ports, and 192.0.2.17 for LAN2 ports. Use the default IP address to access Local Management using a Telnet session. You can establish a Telnet session from a terminal on the router's LAN or across a WAN connection.

Note The default IP address must not be in use by another device on the network or a conflict may occur. The default IP address must not be used as the permanent IP address.

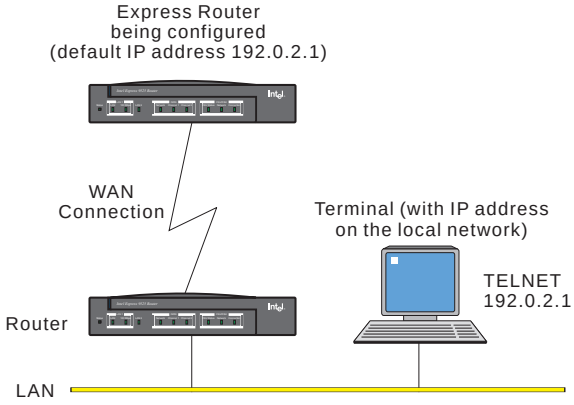
From a terminal on the LAN

Temporarily configure a terminal on the LAN to use the same network number as the default IP address ("192.0.2" is the network number for the default IP address). For example, the terminal could be assigned the IP address 192.0.2.2.



From a terminal across the WAN

Start a telnet session on the default IP address of the router from a remote terminal connected via another router to a WAN port of the Express Router.



Note This is only possible if the default configuration of the WAN port on the Intel Express Router matches the WAN connection type being used.

Local Management Access From the Console Port

Local Management via the console port

From the console port of the router, you can access Local Management by connecting a VT100-compatible terminal or PC running emulation software such as HyperTerminal (HT). The terminal can be connected directly to the console port or through an asynchronous modem connection from a remote location.

In order to use the console port for accessing Local Management, the console port must be configured to the console mode.

Setting the console port to console mode

To set the console port for use with a VT100-compatible terminal or PC, use one of these methods:

From Intel Device View

You set the console port to console mode using Connection Setup.

- From the `Configuration` menu, click `Connection Setup`.
- Double-click the console port to start the port setup.
- Select the `Connection to terminal` check box, then click `Next` > `Finish`.

From Advanced Setup

Advanced Setup is explained in detail in the chapters that follow.

- From the Advanced Setup main display, select `Management` > `Console port`.
- Set the `Console Port Mode` parameter to `Console`.

Using Recovery Mode from the console port

You can force the router console port to console mode using the RUN command from the Recovery Mode command line interface. See “Using the Recovery Mode from the Console Port”, p. 305 for details.

Direct Connection to the Console port

Local Management via a direct terminal connection

To access Local Management using the console port:

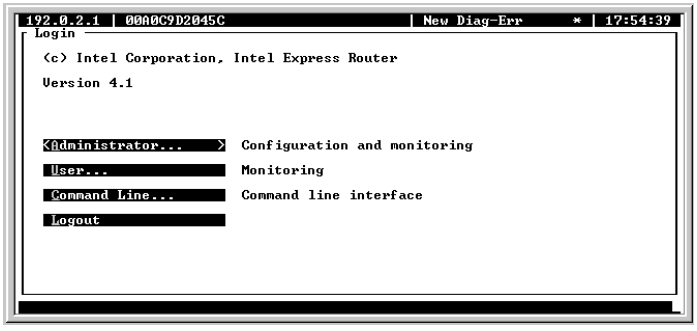
1. Check that the console port is set to console mode.

   See “Setting the console port to console mode” for details.

2. Connect a VT100-compatible terminal to the console port of the router and set the terminal parameters.

   See “Connecting the Console Port to a VT100-compatible Terminal or PC”, p. 30 for details.

3. Press <`Enter`> until the `Login` screen of Local Management is displayed.

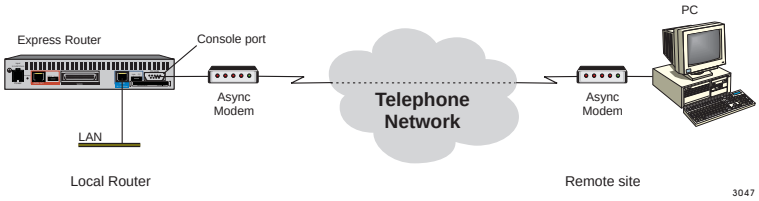


See “Local Management Login”, p. 88.

Dial-in Modem Connection to the Console Port

Local Management via a dial-in modem connection

The console port supports an asynchronous modem connection over the telephone network to a remote VT100-compatible terminal for access to Local Management.



The remote terminal establishes a connection to the router on a dial-in basis using asynchronous communication.

To set up the router and the local modem

To ensure the proper operation, it is important that you perform the steps in the correct order.

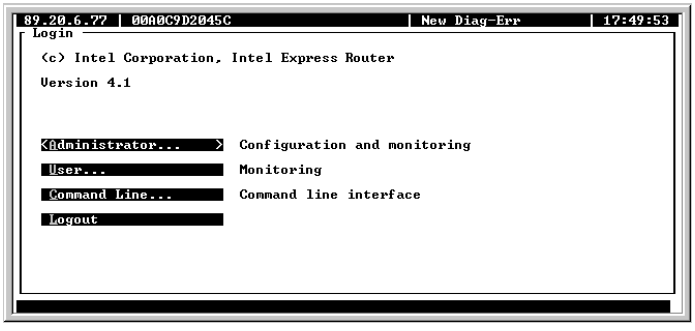
1. Check the console port is set to console mode.
   See “Setting the console port to console mode” for details.
2. Turn off power to the router and modem.
3. Connect the modem to the console port using the terminal cable supplied with the Express Router. Depending on the modem, you may need to use an adapter to terminate the terminal cable to the modem port (adapters are not supplied as an accessory to the router).
4. Connect the modem to the telephone network.
5. Turn on power to modem.
6. Connect power to the router.

To set up the remote terminal and modem

To connect the remote VT100-compatible terminal or PC running terminal emulation software:

1. Connect the terminal or PC to the telephone network via an asynchronous modem.
2. Set the terminal parameters or terminal emulation parameters to:
   - 9600 baud
   - 8 data bits
   - no parity
   - 1 stop bit
   - no flow control
3. Dial-in to the router from the terminal or PC.

   Refer to the terminal or terminal emulation documentation for instructions.
4. At the screen cursor, press <Enter> to access the Local Management Login screen.



See “Local Management Log in” for further instructions.

Local Management Login

Access Restrictions

There are two types of login permissions, `Administrator` and `User`.

Administrator

No access restrictions apply, all configuration and monitor functions are available.

User

Access restrictions apply. Monitor functions are available, but not router configuration.

Note Only one User or Administrator can be logged on to Local Management at a time.

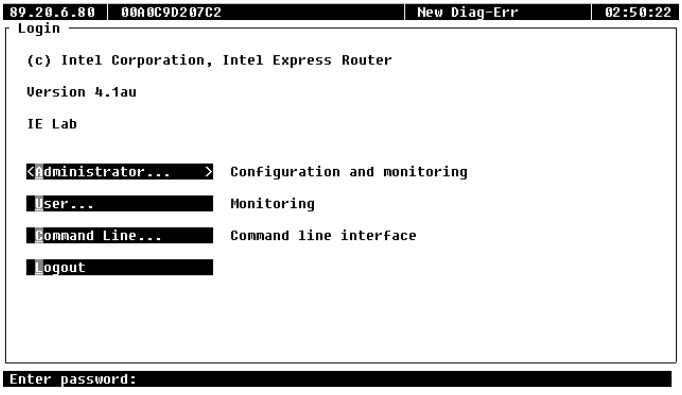
Passwords

You define the login permissions, `Administrator` or `User`, for passwords being used. See “Configuring Local Management Passwords and Access”, p. 250.

To login to Local Management

To log in to Local Management from the `Login` screen:

1 Select either `Administrator`, `User` or `Command Line` and press <`Enter`>.

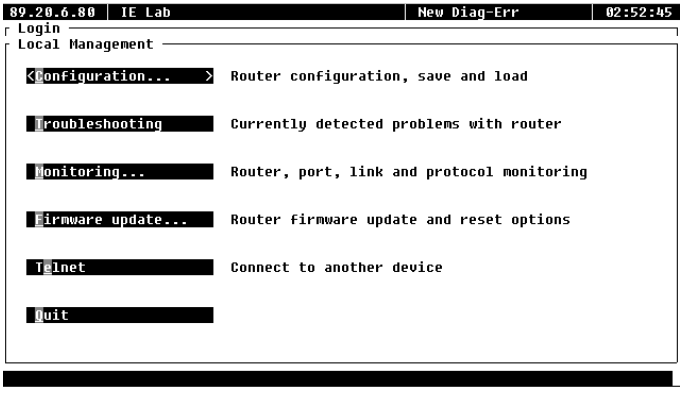


Select `Command Line` to access the command line interface of Local Management. See Chapter “Gas Pump and Command Line Configuration”, p. 259 for details.

2 Type the password and press <Enter>.

If there is no password, press <Enter>. By default no passwords assigned in the router.

After the correct password has been entered, the Local Management main display appears.



Note To make a selection, use the arrow keys to select the option and then press <Enter>, or type the underlined letter of the option.

5 Introduction to Advanced Setup

In this chapter

This chapter describes the general use and features of Advanced Setup. Specific instructions on configuring the router using Advanced Setup are described in the chapters that follow.

Advanced Setup Overview

Advanced Setup

Advanced Setup is a configuration tool that provides complete router configuration capability. The Connection Setup wizards and other configuration programs available in Intel Device View fulfill the configuration requirements for most installations. There are some features or settings that are only available from Advanced Setup. Advanced Setup gives access to all available parameters and allows you to fine-tune setup and router performance.

Advanced Setup is accessible from Intel Device View and Local Management.

Using the Connection Setup wizards after Advanced Setup

There are some parameters available from Advanced Setup but not from the Connection Setup wizards in Intel Device View. If you configure any of these parameters for a specific port or link and then use Connection Setup on the port or link, the parameters are set to their default values.

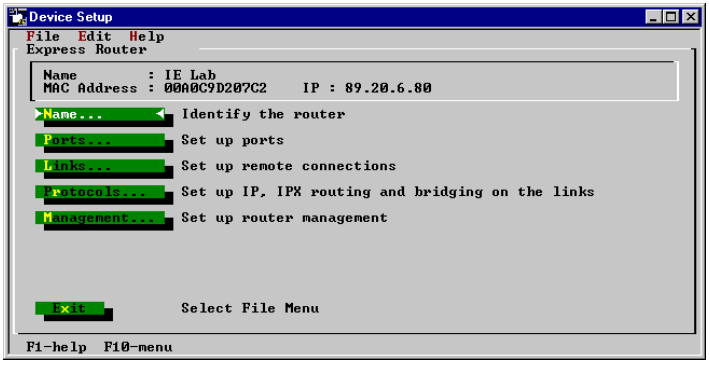
Accessing Advanced Setup

To access Advanced Setup from Intel Device View

To access Advanced Setup from within Intel Device View:

1 Open the router for management in Intel Device View.

2 Select `Advanced Setup` from the `Configuration` menu.

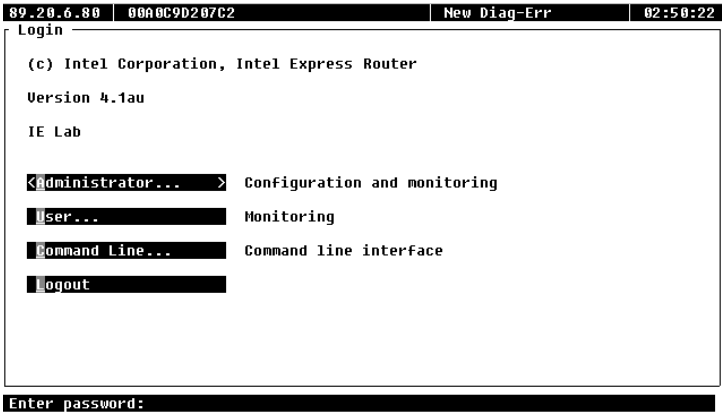


The Advanced Setup main display screen appears.

To access Advanced Setup from Local Management

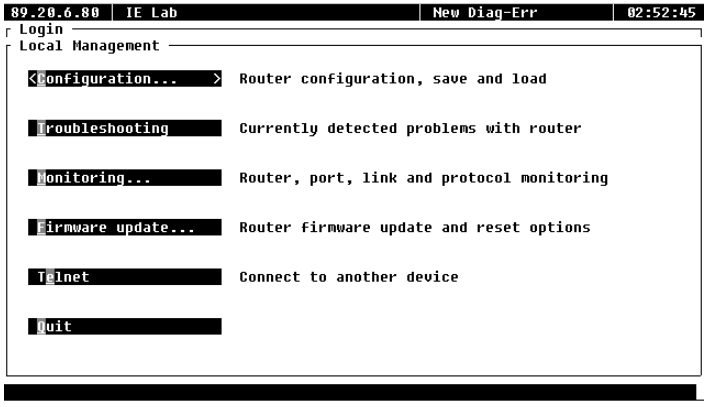
To access Advance Setup in Local Management:

1 Access Local Management on the router using Telnet or the console port.

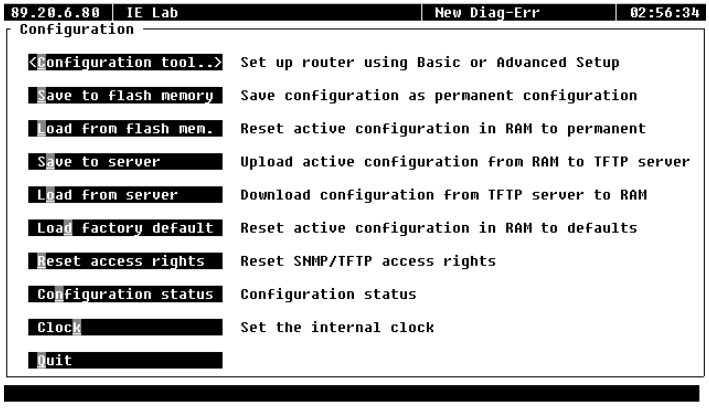


Note The Login screen shows the current firmware version.

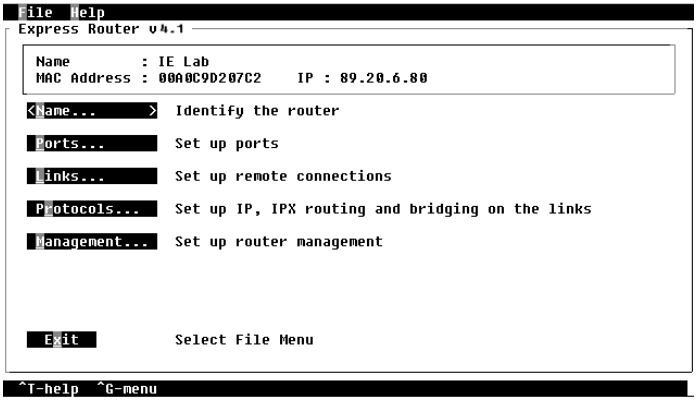
2 Login as `Administrator`.



3 Select `Configuration`.



4 Select `Configuration Tool`.



Advanced Setup overview

The Advanced Setup main display gives access to the following:

Name (optional)

General parameters to describe the router on the network. These parameters can also be configured from Intel Device View, see “Management setup in Intel Device View”, p. 72.

Port (must be configured)

Configure the physical ports on the router to the type of service link for each.

- Use `WAN port` to configure the port for a PPP leased line, Frame Relay or X.25 link.
- Use `CSU/DSU port` to configure the port for a PPP leased line, Frame Relay or X.25 service, and internal CSU/DSU to the T1 service.

Use `Console port` option to configure the console port for connection to an asynchronous modem to provide a PPP dial-up link.

Links (must be configured)

Sets up the logical links to remote sites for the different ports:

- PPP leased lines
- Frame Relay links
- X.25 links

Dial-up modem links to the remote destinations on the console port

- Internet Tunnels.

Note The port must be configured before you can set up the port.

Advanced Setup allows configuration of links to optimize data transfer and control and secure WAN links (data compression, link activity alarms, timers and so on).

Protocols (must be configured)

Use Protocols to setup IP routing and filtering (firewall), IPX routing and Bridging on the LAN and WAN links. Use Links to set up WAN links before you configure the network protocols.

To set up IP routing, IPX routing and Bridging see these chapters:

- Chapter 7 “Configuring IP Routing”, p. 153
- Chapter 8 “Configuring Novell IPX Routing”, p. 203
- Chapter 9 “Configuring Bridging Services”, p. 225.

Management (optional)

Set up the following management services.

- Enable or disable licensed software features using the Value Added Services option.
- Set SNMP, TFTP and Telnet access restrictions for security. SNMP and TFTP are used for management, configuration and firmware updates in the router.
- Define SNMP Trap destinations.
- Disable or enable Local Management access and define passwords.
- Set the console port for use with either a VT100-compatible terminal or modem.
- Configure the messages that appear in the Log System.

On-line Help

On-line help

If you access Advanced Setup from Intel Device View, click a parameter and press the F1 key to get description and explanation of the parameter.

Note This feature is not available when Advanced Setup is accessed from Local Management.

General Configuration

System Parameters - name, location and contact

The optional system parameters identify the router. To access these parameters, click `Name` from the Advanced Setup main display.

Exiting Advanced Setup

Dynamic configuration of the Express Router

The Express Router uses dynamic configuration. Any configuration changes are active in RAM when you select to save when exiting Advanced Setup. To save the configuration permanently, you must save it to flash memory. Otherwise it will be lost following the next restart and the router reverts to its previous configuration.

To exit Advanced Setup

To exit Advanced Setup, select one of these options from the `File` menu:

- Exit <Save data>.

  The new configuration is temporarily stored in the router's RAM and is operational immediately (see the explanation of dynamic configuration).

  This allows you to check the configuration before you save it to flash memory as the permanent configuration.

  Note If the router is restarted before the new configuration is saved, the new configuration is lost.

- Quit (Discard data).

  The changes are discarded. The router uses the existing configuration.

To permanently save a new configuration

To permanently save a new configuration, save it to flash memory:

- From the `Configuration` menu of Intel Device View, click `Save to Flash Memory`.
- From the `Configuration` screen of Local Management, select `Save to flash memory`

If a configuration is saved to flash memory, the previous configuration is lost.

To restore a previous configuration

To restore the previous configuration:

- From the `Configuration` menu of Intel Device View, click `Restore from Flash Memory`.
- From the `Configuration` screen of Local Management, select `Load from flash memory`.

You can also restart the router.

6 Configuring WAN Services and Links

In this chapter

This chapter describes how to configure the Express Router using Advanced Setup.

CSU/DSU and HDSL2 ports

T1 Overview

Full T1 and fractional T1

T1 is supported on HDSL2 and CSU/DSU ports of the router. T1 is a digital signal operating at a line speed up to 1.536 Mbps. The signal is divided into 24 channels operating at bandwidths of 64 kbps or 56 kbps.

A full T1 line utilizes all 24 channels, providing a line speed of 1.536 Mbps (24 x 64 kbps) or 1.344 Mbps (24 x 56 kbps). Fractional T1 does not utilize all 24 channels, and provides a lower line speed at a lower cost. Fractional T1 allows you to purchase the number of channels (1 to 23) to meet your line speed requirements. For example, use four channels at 64 kbps to get a line speed of 256 kbps.

Channel allocation and total line speed

When you configure the router for fractional T1, you must choose the data channels and total line speed to match your T1 service.Your subscription may either allocate specific channels and/or state the total line speed of your service. If specific channels are allocated, you must use those channels. The number of channels determines the line speed. Continuous channels are most commonly allocated and selected as default.

Configuring a CSU/DSU Port

CSU/DSU ports

Express Routers with CSU/DSU ports have an internal CSU/DSU unit to connect directly to a full T1 or fractional T1 line. The CSU/DSU requires configuration in accordance with the provided T1 service. Use the configured CSU/DSU port to connect to a PPP leased line, a Frame Relay network, or X.25 network.

For more information about the CSU/DSU port and T1 technology, see the Reference Manual.

Line coding and channel speed considerations

The Express Router supports AMI and B8ZS line coding. B8ZS is most common and default. Obtain the line coding from your service subscription or use B8ZS.

B8ZS line coding supports channel speeds of both 64 and 56 kbps. AMI line coding supports only 56 kbps channel speed.

Note Do not configure the router for AMI line coding and 64 Kbps channel speed.

Framing format and channel speed considerations

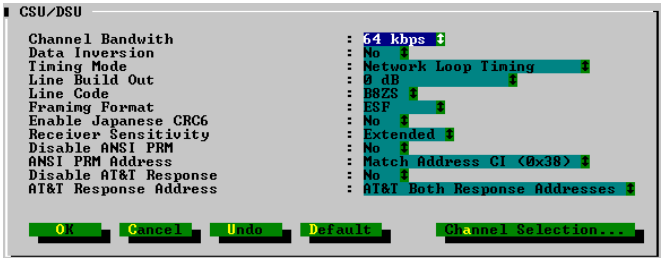
The Express Router supports ESF and D4 framing format. ESF is most common and the default. Use D4 framing only when it is stated in your service subscription.

Note Do not configure the router for D4 framing and 64 Kbps channel speed.

To configure the CSU/DSU port

To configure the CSU/DSU port to your T1 service:

1 From the Advanced Setup main display, select `Port> CSU/DSU Port` > `Configure CSU/DSU`.



2 Configure the CSU/DSU parameters to your service subscription. The following parameters must be configured: `Channel Bandwidth`, `Line Code`, and `Framing Format`. The default settings for the remaining parameters are suitable for almost all installations and usually do not require changing.

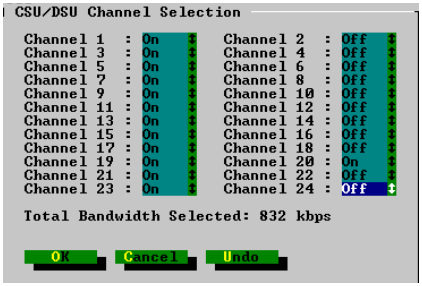
Parameter	Description
`Channel Bandwidth`	Sets the channel speed for the line. `64 kbps` is default and suitable for most installations. Use `56 kbps` only when the T1 interface to this router has AMI line coding or the remote link is configured for 56 kbps.
`Line Code`	Defines the signal coding. Choose between `AMI` and `B8ZS`. `B8ZS` (default) works for most installations. Use `AMI` only if it is stated in the service subscription. Do not configure for AMI line coding and 64 Kbps line speed.
`Framing Format`	Defines the frame coding `D4` or `ESF`. `ESF` is default and works for most installations. Select `D4` only if it is stated in your service subscription. Do not configure the router for `D4` framing and `64 Kbps` channel speed.
`Data Inversion`	Sets the CSU/DSU to invert the transmitted data and receive inverted data. Uninverted is the default setting and works for most installations. Select Inverted only if it is specifically stated in the service subscription.

Parameter	Description
`Timing Mode`	The CSU derives its timing signal from the receive data. This is known as network loop timing. `Network loop timing`, the default setting, is suitable for most installations. Use `Master` timing only for leased line applications when it is known that this router supplies the timing signal.
`Line Build Out`	Sets the line attenuation. The values are based on the length of the line from the router to the network switch. 0 db, the default, works for most installations.

In most cases, do not change the following parameters from default. Changing these parameters may have unintended consequences.

Parameter	Description
`Enable Japanese CRC6`	Enables the Japanese version of CRC6 for Japanese transmission systems. No is default.
`Receiver Sensitivity`	Extends the sensitivity of the receiver for weak line applications. Normal is default.
`Disable ANSI PRM`	Disables sending and receiving of ANSI T1.403 Performance Report Messages (PRM). No is default.
`ANSI PRM Address`	Applicable only when ANSI is enabled, used to set the match address. CI (0x38) is default.
`Disable AT&T Response`	Disables the CSU/DSU response to AT &T 62411 loopstyle commands received on the line. No is default.
`AT&T Response Address`	Applicable only when AT&T Response is enabled. Both is default.

3 To configure total line speed and channel allocation, select `Channel Selection`. This option configures the line for full T1 (all 24 channels) or fractional T1.

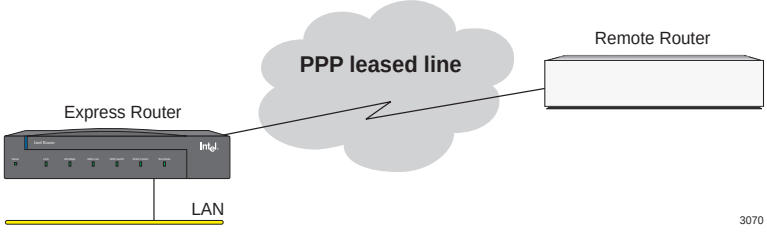


Select the required channels by setting them to `ON` until the `Total Bandwidth Selected` value matches the line speed of your subscription.

Configuring for PPP Leased Lines

PPP leased lines

PPP leased lines are supported on WAN and CSU/DSU ports.



An overview of the features supported by PPP is given in “Point-to-Point Protocol (PPP)”, p. 15.

Configuration overview

The following shows an overview of how a PPP leased line is set up in the router:

Port (physical port on router)		
PPP leased line		
IP Routing	IPX Routing	WAN Bridging

The PPP leased line must be configured and then the routing protocols (IP and Novell IPX) and bridging are configured on top of the link.

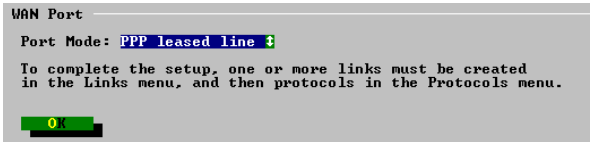
To configure a PPP leased line

Follow this procedure to configure a PPP leased line on an WAN or CSU/DSU port.

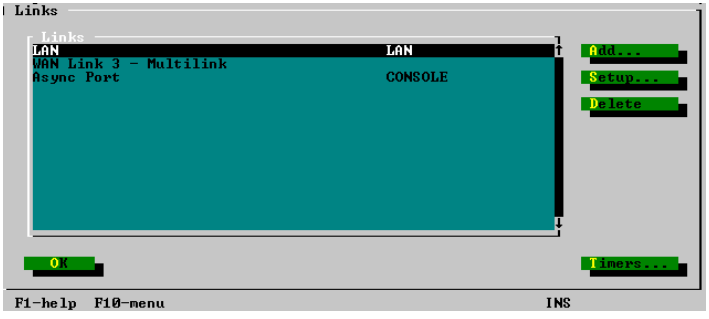
Note The WAN2 and CSU/DSU ports are configured for PPP leased line operation by default and you may not need to configure the WAN link further, see “Router Factory Default Setup”, p. 21.

1 Configure the WAN service for the port to PPP leased line.

- From the Advanced Setup main display, select `Port` and then the appropriate port from the menu.
- Set the `Port Mode` parameter to `PPP leased line` and select OK.

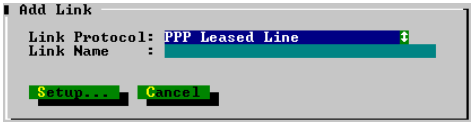


2 From the Advanced Setup main display, select `Links`.



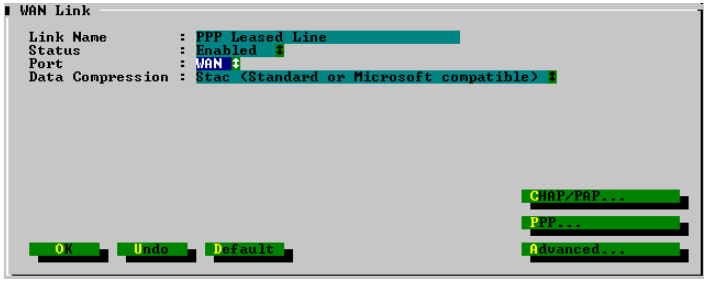
- To configure a new link, select `Add` and go to step 3.
- To edit an existing link, select the link and then select `Setup`. Go to step 4.

3 From the `Add Link` screen, set the `WAN Protocol` field to `PPP Leased Line`, and enter a name for the link.



Select `Setup` to continue.

4 From the WAN Link screen, configure the PPP leased line link parameters to your requirements.



The parameters are:

Parameter	Description
`Status`	Enables and disables link.
`Port`	Select the port on which the link is to be added.
`Data compression`	Selects data compression to improve transmission over the link. Must be enabled on both routers over the link or compression will not be used.

Note In most cases, the parameters available from the PPP option on the `WAN Links` screen do not require configuring and the default values can be used.

5 If link security using CHAP or PAP is required, select `CHAP/PAP` on the `WAN Link` screen. See “Configuring Password Protection using CHAP or PAP”, p. 144 for details.

6 Select `Advanced` on the `WAN Link` screen to set up any advanced link features required.

See “Configuring Advanced Link Features and Parameters”, p. 146 for a description of the advanced link features available.

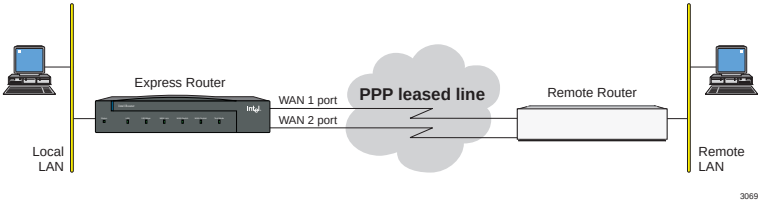
7 Select the `Protocols` option of Advanced Setup to configure routing as required.

See Chapter 7 “Configuring IP Routing”, p. 153, Chapter 8 “Configuring Novell IPX Routing”, p. 203 and Chapter 9 “Configuring Bridging Services”, p. 225.

Configuring a PPP Leased Line Multilink

PPP Leased Line Multilink

The Express 9535 Router supports a PPP leased line Multilink connection using the two WAN ports. The PPP Multilink logically combines two leased line connections to a remote destination into a single connection, essentially doubling the transmission bandwidth.



To create a multilink, the individual leased lines must operate at the same transmission speed.

Configuration overview

The following shows an overview of how a PPP leased line Multilink is set up in the router:

WAN1 port		WAN2 port
PPP leased line		PPP leased line
PPP Multilink		
IP Routing	IPX Routing	WAN Bridging

Configure each port for a PPP leased line connection and then configure the PPP Multilink. Configure the routing protocols (IP and Novell IPX) and bridging on top of the Multilink.

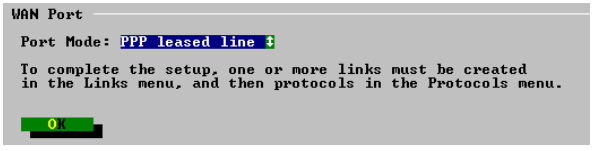
Note Before you can configure a PPP leased line Multilink, existing single PPP leased line links must be deleted.

To configure a PPP Leased Line Multilink

Follow this procedure to configure a PPP leased line Multilink.

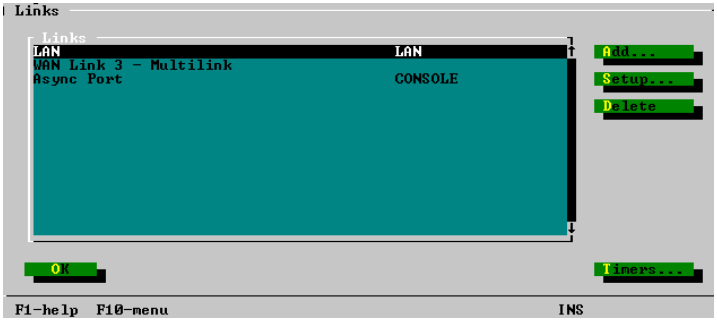
1 Configure the two WAN ports for PPP leased line.

- From the Advanced Setup main display, select `Port` > `Wan Port1`.
- Set the `Port Mode` parameter to `PPP leased line`.



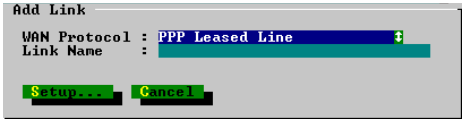
- Repeat this step for the WAN2 port.

2 From the Advanced Setup main display, select the `Links` option.



- To configure a new link, select `Add`.
- To edit an existing link, select the link and then select `Setup`. Go to step 4.

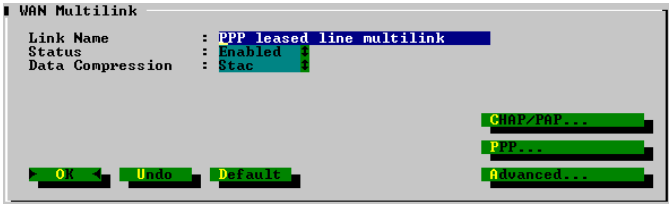
3 From the `Add Link` screen, set the `WAN Protocol` field to `WAN Multilink PPP`, and enter a name for the link.



Note If a single PPP leased line link exists, you cannot add a Multilink until you delete the existing link.

To continue, select `Setup`.

4 Configure the PPP leased line link parameters to your requirements.



The parameters are as follows.

Parameter	Description
`Status`	To enable and disable link.
`Data compression`	Selects data compression to improve transmission over the link. This must be enabled on both routers over the link or compression will not be used.

Note In most cases, the parameters available from the PPP option on the `WAN Links` screen do not require configuring and the default values can be used.

5 If link security using CHAP or PAP is required, select `CHAP/PAP` on the `WAN Link` screen. See “Configuring Password Protection using CHAP or PAP”, p. 144 for details.

6 On the `WAN Link` screen, select `Advanced` to set up any advanced link features required.

See “Configuring Advanced Link Features and Parameters”, p. 146 for a description of the advanced link features available.

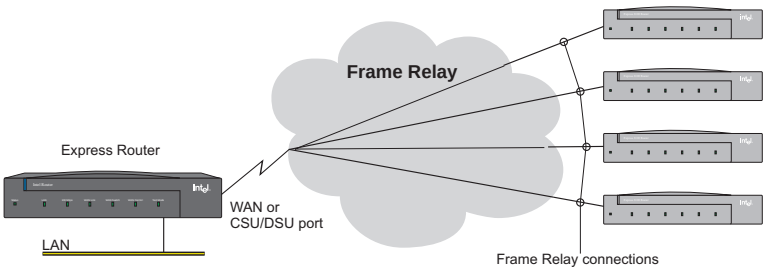
7 From the Advanced Setup main display, select the `Protocols` option to configure routing as required.

See Chapter 7 “Configuring IP Routing”, p. 153, Chapter 8 “Configuring Novell IPX Routing”, p. 203 and Chapter 9 “Configuring Bridging Services”, p. 225.

Configuring Frame Relay Services

Frame Relay

Frame Relay is supported on WAN ports and CSU/DSU ports. Frame Relay supports multiple simultaneous logical links (Permanent Virtual Circuits) across a single physical link (see “Supported Connections”, p. 331 for details). Frame Relay virtual circuits are always available for data communications; call setup is not required.



Flow Control

You can configure the following flow control features in the Express Router.

Note For more detailed explanation of Flow Control and its parameters, see the Intel Express Router Reference Manual.

Avoid congestion using BECN

The router supports Backward Explicit Congestion Notification (BECN). The BECN feature reduces the risk of lost packets. This is especially favorable when using data compression, which is highly sensitive to packet loss.

When the Frame Relay switch detects congestion in the Frame Relay network, it sends out a Backward Explicit Congestion Notification, or BECN. When the router receives a BECN, it reduces its transmission rate by 25%. This continues at intervals until BECNs are no longer received. The transmission rate is then gradually increased.

Traffic distribution control using bandwidth weights

The Express Router allows you to control the distribution of data traffic between links (DCLIs) on the Frame Relay port through the use of bandwidth weights. A bandwidth weight is a number assigned to a link to determine the fraction of the total available bandwidth allotted to the link when active, equal to:

$$\frac{\text{bandwidth weight of the link}}{\text{sum of bandwidth weights for all active links on the port}}$$

Example

If there are 3 links (named A, B and C) that have bandwidth weights of 1, 4, and 5 respectively.

- When there is traffic on links A and B, link A receives 1/5 of the bandwidth and link B receives 4/5 of the bandwidth.
- When there is traffic on links B and C, link B receives 4/9 of the bandwidth and link C receives 5/9 of the bandwidth.
- When there is traffic on links A, B and C, link A receives 1/10 of the bandwidth, link B receives 4/10 of the bandwidth and link C receives 5/10 of the bandwidth.

Note Bandwidth weighting takes effect only when the port is utilized 100%. If there is traffic on only one link, that link receives 100% of the bandwidth.

Maximum Transfer Rate

You can configure a maximum transfer rate for each link (DLCI) on the port. You define your own value or have the rate calculated from the Committed Information Rate (CIR), the Command Burst size (Bc) and the Excess Burst size (Be) parameters, where:

Maximum transfer rate = CIR * (1+Be/Bc)

These parameters are provided by your service provider.

Default Frame Relay set-up

Frame Relay services are configured by default for WAN ports and CSU/DSU ports. By default, the router automatically detects the Frame Relay switch type (LMI type or DLCMI) and the Frame Relay links (DLCIs) in your Frame Relay subscription. The router configures the detected Frame Relay links with default routing of IP (RIP-1) and IPX. This allows you to remotely configure your router over a Frame Relay link after the router hardware is installed.

Configuration overview

The following shows an overview of how Frame Relay links and services are set up in the router:

<table>
<tr><td colspan="4">Port configured for Frame Relay</td></tr>
<tr><td colspan="3">Frame Relay link</td><td rowspan="2">additional links</td></tr>
<tr><td>IP Routing</td><td>IPX Routing</td><td>WAN Bridging</td></tr>
</table>

You must first configure the port to Frame Relay port, then you can begin adding Frame Relay links. The routing protocols (IP and Novell IPX) and bridging are then configured on top of the Frame Relay links as required.

Automatic Configuration of Frame Relay Service

Automatic configuration of Frame Relay services and links

The router can be set up to automatically detect the Frame Relay LMI Type and Frame Relay Links (DLCIs) from your subscription. The links are configured for routing according to a default routing scheme you define.

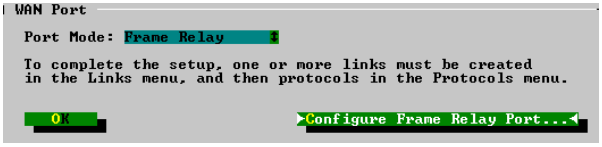
Note The router continually autodetects the Frame Relay LMI type and DLCIs of your subscription. Links no longer detected are automatically deleted along with their configuration.

You can disable this feature on a individual link basis. See “Manual Configuration of Frame Relay Services and Links”, p. 113.

To configure Frame Relay services and links automatically

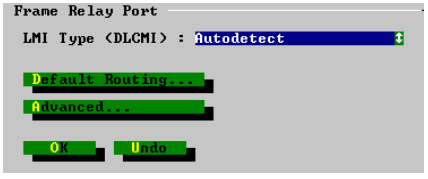
To configure the autodetection of Frame Relay services and establish default routing and bridging over logical links through the Frame Relay network.

1 From the Advanced Setup main display, select the `Port`, then select the port you want to configure.



2 Set the `Port Mode` parameter to `Frame Relay`.

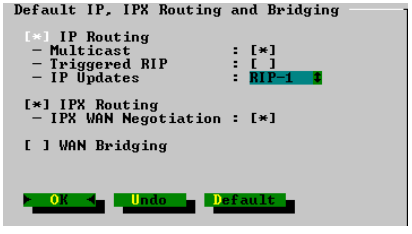
3 Select `Configure Frame Relay Port`.



4 Set the `LMI Type (DLCMI)` parameter to `Autodetect`.

In most cases, the parameters on the `Advanced` screen do not require configuring and their default values should be used.

5 From the Frame Relay Port screen, select `Default Routing`.



Configure the default routing parameters. The default settings are used on all Frame Relay links detected in your Frame Relay subscription.

Parameter	Description
`IP Routing`	Enables or Disables IP Routing over the Frame Relay links. IP routing is described in Chapter 7 “Configuring IP Routing”, p. 153.
IPX Routing	Enables or Disables IPX Routing over the Frame Relay links. IPX routing is described in Chapter 8 “Configuring Novell IPX Routing”, p. 203.
WAN Bridging	Enables or Disables bridging over the Frame Relay links. Bridging services are described in Chapter 9 “Configuring Bridging Services”, p. 225.

6 To configure advanced features and routing protocols for specific links detected, refer to“To configure a Frame Relay link manually”, p. 114 for details.

See “Configuring Advanced Link Features and Parameters”, p. 146 for a description of the advanced link features available.

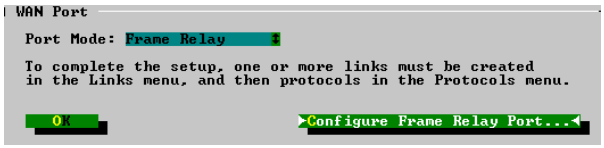
Manual Configuration of Frame Relay Services and Links

To configure Frame Relay services on a port

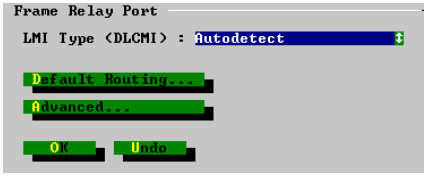
To configure Frame Relay services on a port:

1 From the Advanced Setup main display, select the `Port`, then select the port you want to configure.

2 Set the `Port Mode` parameter to `Frame Relay`.



3 Select `Configure Frame Relay Port`.



4 Set the `LMI Type (DLCMI)` field to the DLCMI type noted in your Frame Relay subscription.

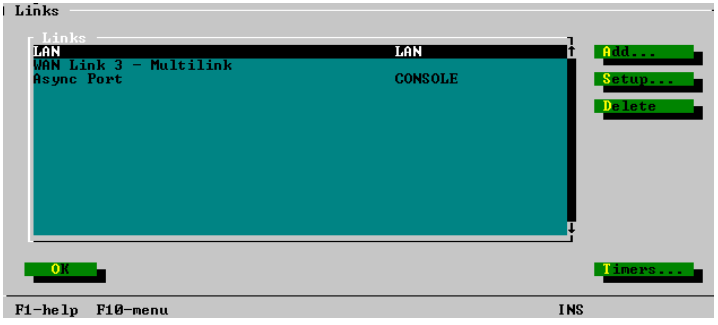
Note If you set this parameter to `Autodetect`, the router will automatically detects and configures the Frame Relay switch type (DLCMI) and links (DLCIs) in your Frame Relay subscription. See “Automatic Configuration of Frame Relay Service”, p. 111.

In most cases, the parameters on the `Advanced` screen do not require configuring and their default values should be used.

To configure a Frame Relay link manually

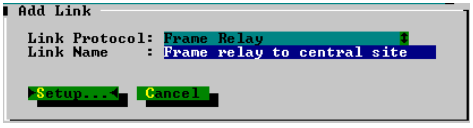
To add or edit a Frame Relay link:

1 From the Advanced Setup main display, select the `Links` option.



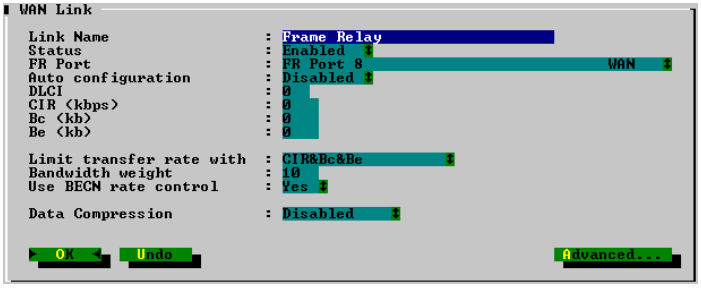
- To configure a new link, select `Add`.
- To edit an existing link, select the link and then select `Setup`. Go to step 3.

2 From the `Add Link` screen, set the `Link Protocol` field to `Frame Relay`. If you are configuring an IDSL link, set the parameter to Frame Relay/IDSL.



Select `Setup` to continue.

3 From the `WAN Link` screen, configure the Frame Relay link parameters to your requirements.



The DLCI parameter must be configured. Configure the other parameters as needed.

Parameter	Description
`Status`	Used to enable or disable the link.
`FR Port`	Selects the Frame Relay port to which the link is assigned. (This is not available for Frame Relay/IDSL links).

Parameter	Description
Auto configuration	Enables or disables the autoconfiguration as defined by the autodetect feature for the port (see "Automatic configuration of Frame Relay services and links", p. 111). When Enabled, the link is automatically configured to the default routing and is automatically deleted if removed from your subscription. When Disabled, the link is not automatically configured or deleted. This parameter must be set to Disabled to manually configure routing protocols.
DLCI	Data Link Connection Identifiers (DLCIs) are used in Frame Relay networks to identify links to different remote sites. Enter the appropriate DLCI here from your Frame Relay subscription.
CIR	The Committed Information Rate (CIR) is the data throughput rate the service provider commits to provide on the line. This is the lower limit when adjusting the maximum transfer rate. Default is zero.
Bc	The Committed Burst (Bc) is the maximum number of bits a service provider agrees to transfer over a measured time interval: Bc = CIR * time (seconds). Default is zero. If CIR is non-zero, then Bc must be non-zero.
Be	The Excess Burst (Be) is the maximum number of bits the service provider agrees to transfer in addition to the Committed Burst size. Default is zero. If CIR is non-zero, then Be must also be non-zero.
Maximum Transfer Rate	Defines the data transfer limit (kbps) for traffic on the link as supplied by the service provider. Available for selection only when the Limit Transfer Rate is set to Maximum Transfer Rate.

Parameter	Description
`Limit transfer rate with`	Defines whether the maximum transfer rate used on the link is determined by the `Maximum Transfer Rate` parameter or calculated using the `CIR`, `Bc` and `Be` where: maximum transfer rate = CIR* (1+Be/Bc) **Note:** If CIR, Bc and Be are zero, then the transfer rate is limited by the bandwidth of the port (line speed of your service).
`Bandwidth weight`	Determines how large a share of the bandwidth the link is allotted when active, relative the other active links on the port. The bandwidth weight only takes effect when the port is 100% utilized.
`Use BECN rate control`	Defines the use of BECNs received from the Frame Relay Switch.
`Data Compression`	Enables or disables data compression. Must be enabled in both routers over the Frame Relay link or compression will not be used.
`Port Speed`	This parameter is available for IDSL Frame Relay links only. This defines the line speed for your link. This must match your service subscription. 64kbps uses a single B-channel. 128 kbps uses the two B-channels. 144 kbps uses the two B-channels and the D-channel and is available for ISDN U ports only

4 Select `Advanced` on `WAN Link` screen to set up any advanced features required.

See “Configuring Advanced Link Features and Parameters”, p. 146 for a details on the remaining parameters.

5 Select the `Protocols` option of Advanced Setup to configure IP routing, IPX routing and bridging on the Frame Relay link.

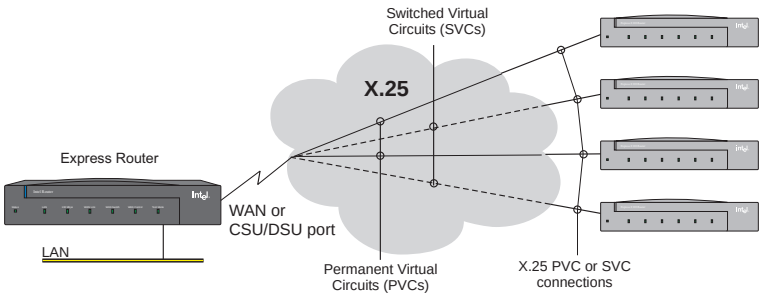
Note The Auto configuration parameter on the WAN Link screen must be set to Disabled.

See Chapter 7 “Configuring IP Routing”, p. 153, Chapter 8 “Configuring Novell IPX Routing”, p. 203 and Chapter 9 “Configuring Bridging Services”, p. 225.

Configuring X.25 Services

X.25

X.25 is available for use via WAN and CSU/DSU ports on the Express Router. X.25 supports multiple simultaneous logical channels, Permanent Virtual Circuits and Switched Virtual Circuits, across a single physical interface (see “Supported Connections”, p. 331 for details). Permanent Virtual Circuits (PVCs) are always available for data communications; call setup is not required. Switched Virtual Circuits (SVCs) are only established when data requires transmitting.



Before the router can use X.25 service, the port must be configured as an X.25 port.

Data security over X.25 links

To add the security features supported by PPP (CHAP and PAP) to X.25 links, configure Internet Tunnels on the X.25 links. See “Application of Internet Tunnels for data security over X.25 links”, p. 143.

Configuration overview

The following shows an overview of how X.25 links and services are set up in the router:

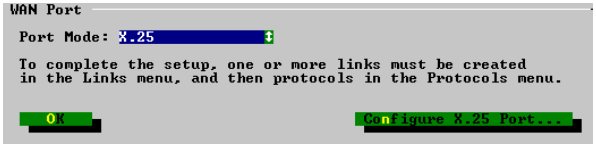
<table>
<tr><td colspan="4">WAN port or CSU port configured for X.25</td></tr>
<tr><td colspan="3">X.25 link (PVC or SVC)</td><td rowspan="2">additional links</td></tr>
<tr><td>IP Routing</td><td>IPX Routing</td><td>WAN Bridging</td></tr>
</table>

A port must first be configured as an X.25 port. The X.25 links (both PVCs and SVCs) are then configured on the X.25 port, followed by the routing protocols (IP and Novell IPX) and bridging on top of the links as required.

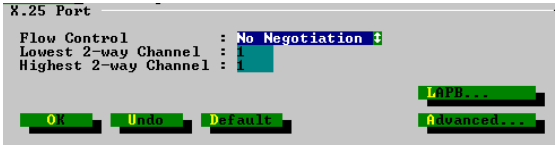
To configure a WAN port or CSU/DSU port for X.25 service

Follow this procedure to configure a X.25 service on a WAN port or CSU/DSU port to your service subscription. The port must be configured before any links are added.

1 From the Advanced Setup main display, select `Port`, then select the appropriate port.



2 Set the `Port Mode` to `X.25` and then select `Configure X.25 Port`.



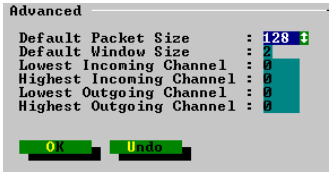
3 Set the `Flow Control`, `Lowest 2-way Channel` and `Highest 2-way Channel` parameters on the `X.25 Port` screen to match your X.25 subscription.

Note Flow Control is sometimes available as an additional service for use over X.25 networks and must be requested from your X.25 network provider.

In most cases, the parameters on the `LAPB` screen do not

require configuring and their default values should be used.

4 Select `Advanced` on the `X.25 Port` screen.

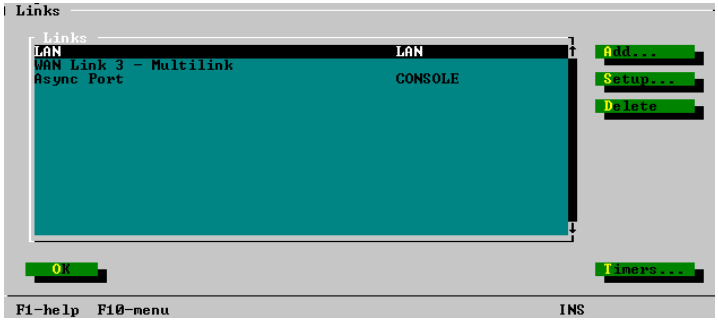


The `Default Packet Size` and `Default Window Size` parameters are only displayed if `Flow Control` is set to `No Negotiation` on the X.25 Port screen.
Set the parameters on the `Advanced` screen for the X.25 Port to match your X.25 subscription.

To configure links over X.25

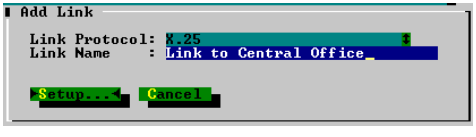
To add or edit links on a port configured for X.25 service:

1 From the Advanced Setup main display, select the `Links` option.



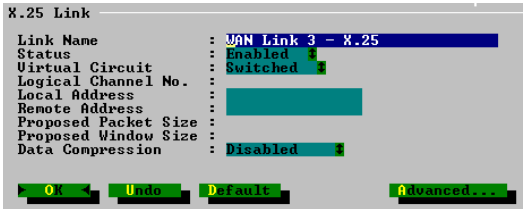
- To configure a new link, select `Add`.
- To edit an existing link, select the link and then select `Setup`. Go to step 3.

2 From the `Add Link` screen, set the `WAN Protocol` field to `X.25`, and enter a name for the link.



Select `Setup` to continue.

3 From the `X.25 Link` screen, configure the parameters for your X.25 link.



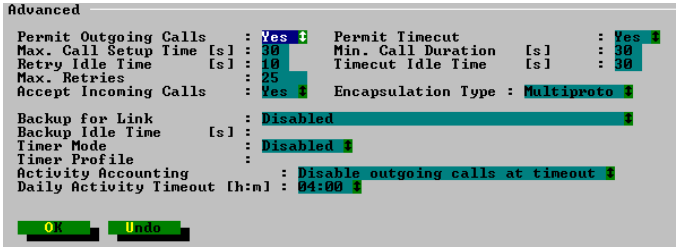
The parameters on the that must be configured are:

Parameter	Description
`Virtual Circuit`	This parameter determines whether the X.25 link is a Permanent Virtual Circuit (PVC) or a Switched Virtual Circuit (SVC). The circuit type should be noted in your X.25 subscription.
`SVC parameters`	For SVCs, the `Local Address` of this router (from your X.25 subscription) and the Remote Address of the router over the X.25 must be configured.
`PVC parameters`	For PVCs, the `Logical Channel Number` must be configured using a unique channel number from your X.25 subscription. The `PVC Packet` and `Window Size` must be configured to match the sizes noted in your X.25 subscription.
`Data compression`	Must be enabled in both routers over the X.25 link or compression will not be used. Data compression should not be enabled on X.25 links faster than 256 kbps (combined bandwidth for all the X.25 links). Compression may reduce the throughput otherwise.

Parameter	Description
`Reverse charging`	Reverse charging must be available in your subscription to the X.25 network before it can be used. If reverse charging is enabled on the link, the remote device must also support reverse charging and be configured for complementary operation. That is, if this router is configured to request reverse charging, the remote device must accept reverse charging.
RPOA	Recognized Private Operator Agency (RPOA) parameter is used to select the X.25 networks to be traversed to the destination. A network is represented by a 4 digit number called a Data Network Identification Code (DNIC). These networks are negotiated with your service provider and should be found in your subscription. You can configure up to 10 DNICs. Separate each entry with a space. Networks are traversed in the order they are entered. If you are not using DNICs leave this parameter blank.

The other parameters can be configured to your requirements.

4 Select `Advanced` on the `WAN Link` screen to set up any advanced link features and parameters.



Set the `Encapsulation Type` parameter to `IP-only` if communicating with IP equipment that only conforms to RFC 877 encapsulation, or is only used for IP routing. Set this parameter to `IPX-only` if transmitting only IPX packets. The `IP-` and `IPX-only` encapsulation protocols save a few bytes in the transmission overheads over the multi-protocol encapsu-

lation method. The Multi-protocol (`Multiprotocol`) setting, which is default, forwards all packet types but uses an extra few bytes of bandwidth per packet sent because of the longer header.

The `Backup for Link` parameter is available for Virtual Switched Circuits. This assigns the link as a backup for other links in case that link fails.

See “Configuring Advanced Link Features and Parameters”, p. 146 for a description of the other advanced link features available.

5 Select the `Protocols` option of Advanced Setup and configure IP routing, IPX routing and bridging on the X.25 link as required.

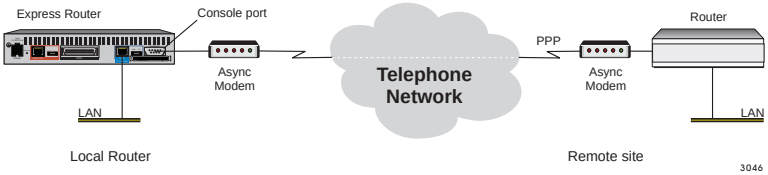
See Chapter 7 “Configuring IP Routing”, p. 153, Chapter 8 “Configuring Novell IPX Routing”, p. 203 and Chapter 9 “Configuring Bridging Services”, p. 225.

Configuring PPP Dial-up Modem Links on the Console Port

Overview

PPP dial-up modem links

The console port of the router supports PPP dial-up links over a normal telephone network using an asynchronous modem. All the facilities offered by PPP links are available, such as data compression, CHAP/PAP, and call-back.



For a list of supported modems, see‘Supported Modems’, p.329.

Multiple logical links

The console port can support multiple logical links to remote destinations. If there is more than one link, the links can only be used to dial-out because it is not possible to identify the incoming call. You must configure all links not to accept incoming calls. Configure this option by using the `Advanced` options accessed from the `WAN Async Link` screen.

Configuration overview

The following shows an overview of how dial-up PPP modem links on the console port are configured.

Console port with asynchronous modem installed			
PPP modem link			additional links
IP Routing	IPX Routing	WAN Bridging	

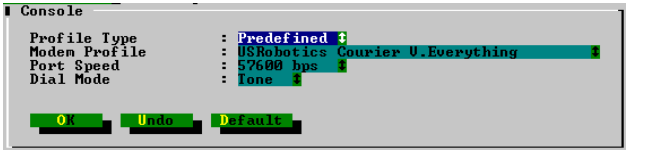
The console port must be configured for the connected modem. The links are then configured, followed by the configuration of the routing protocol (IP, IPX, Bridging) as required.

Configuring the Console Port for the Modem and the PPP Dial-up Links

To configure the console port for your modem

Follow this procedure to configure the console port for the modem.

1 From the Advanced Setup main display, select `Ports` > `Console Port` > `Console`.



2 Set the `Profile Type` to `Predefined` or `Custom`.

This changes the list of modem profiles from which you can chose. See‘Modem Profiles’, p.128. `Predefined` is default.

3 Select the Modem Profile for the modem.

A modem profile marked "(slow)" sets the modem transmission speed to 14,400 bps. Select this only if the router is experiencing transmission problems or you suspect that WAN link transmission is relatively slow.

4 Set the remaining parameters as required:

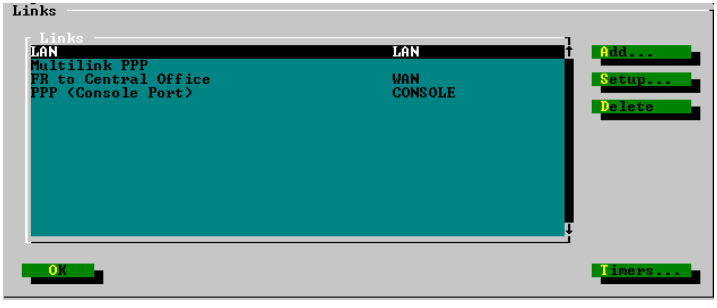
Parameter	Description
`Port Speed`	This is the data transmission speed between the router console port and the modem. In most cases, choose a value equal to or greater than the modem speed. `Max` is the default.
`Dial Mode`	Type of dial system implemented by the telephone network. `Tone` is the default.

To configure a PPP dial-up link

Follow this procedure to configure a PPP dial-up link via a modem on the console port.

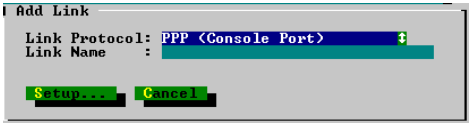
Note When you have completely configured and enabled a PPP dial-up link, the console port is automatically configured to the modem mode. Once in the modem mode, you do not have the ability to configure the router via the console port.

1 From the Advanced Setup main display, select `Links`.



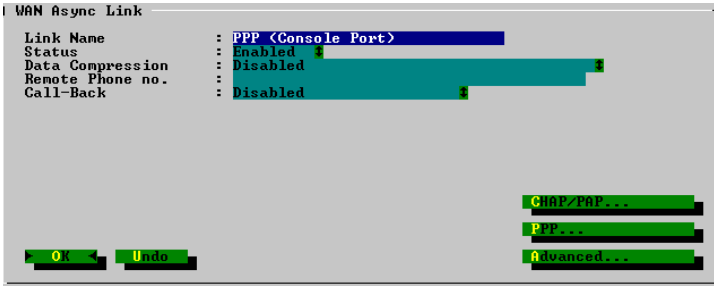
- To add a new link, select `Add`.
- To edit an existing link, select the link and then select `Setup`. Go to step 3.

2 From the `Add Link` screen, set the `Link Protocol` parameter to `PPP <Console Port>` and enter a name.



Select `Setup` to continue.

3 Set the link parameters on the `WAN Async Link` screen.



The following parameters must be configured.

Parameter	Description
`Status`	To enable or disable the link.
`Data Compression`	To enable or disable data compression. Data compression must be enabled in both routers over the link or compression will not be used.
`Remote - Phone No.`	The telephone number of the remote device over the link.

Parameter	Description
`Call-Back`	To enable or disable call-back over the link. Call-back must be configured in the remote site for proper operation. Set to `Request call-back` if the remote is configured to accept call-back requests; the remote site reestablishes the link and receives the charges. Set to `Call Back When Requested` to accept call-back requests. This router reestablishes the link and receives the charges. Set to `Always Call Back` and this router establishes links on a call-back basis only.

In most cases, the PPP-specific parameters accessed from the `PPP` option do not require configuration and you should use the default values.

4 If link security using CHAP or PAP is required, select `CHAP/PAP` on the `WAN Async Link` screen. See‘Configuring Password Protection using CHAP or PAP’, p.144.

5 To configure any advanced features for the link, select `Advanced`.

Note If you have more than the one link configured over the console port, set `Accept Incoming Calls` to `NO`.

See ‘Configuring Advanced Link Features and Parameters’, p.146 for a description of the advanced parameters.

To set the console port to modem mode

The console port has two operating modes, Console and Modem. For modem links, the console port must be in Modem mode. This is done automatically after you add a PPP dial-up link to the console port. To manual configure the console port to Modem mode:

1 From the Advanced Setup main display, select `Management > Console Port`.

2 Set the `Console Port Mode` to `Modem`.

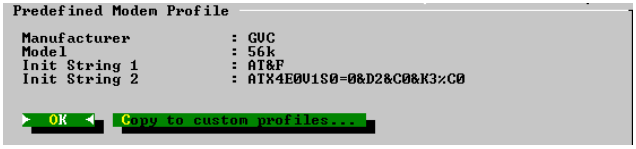
Note While in the Modem mode, you are unable to configure the router using Local Management via the console port. Before you are able to Telnet to the router,

you must wait for the Telnet timeout period to expire (see “Configuring Local Management Passwords and Access”, p. 250).

Modem Profiles

Modem Profiles

A Modem Profile contains necessary configuration data to set up the console port for the connected asynchronous modem. The profile contains the manufacturer name and model of the modem, along with a set of initialization strings (AT commands) to configure the router for operation with the modem.



Predefined Profiles

Predefined modem profiles are available for all supported modems. Predefined profiles contain the necessary information to set up the console port for the chosen modem and do not require any modification. See Appendix B, “Supported Modems”, p. 329 for details on supported modems and explanation of initialization string commands

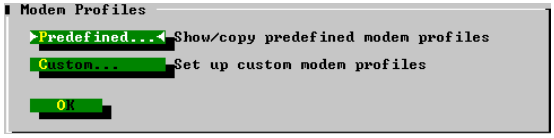
Custom Profiles

Custom Profiles are user-defined profiles. You can create a completely new profile or edit a Predefined Profile. If you are going to use a Custom Profile, it is recommended that you base it on a Predefined Profile. Use the Copy option to perform this operation.

To copy a Predefined Modem Profile as a Custom Profile

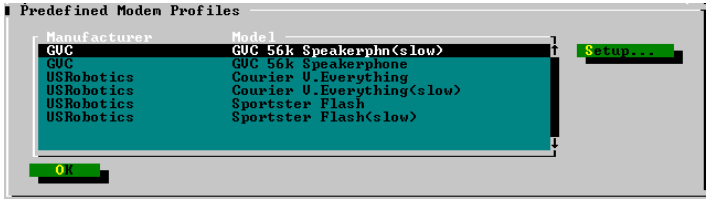
Copying a predefined profile as a custom profile allows you to edit the predefined profile to suit your requirements.

1 From the Advanced Setup main display, select `Port` > `Console Port` > `Modem Profiles`.

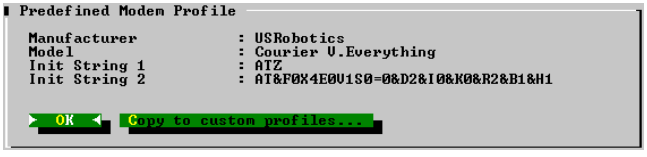


Select `Predefined`.

2 Select the model of your modem from `Predefined Modem Profiles` list and then select `Setup`.



3 Select `Copy to custom profiles`.



The profile is added to the Custom Profile list. You can edit the profile to suit your requirements.

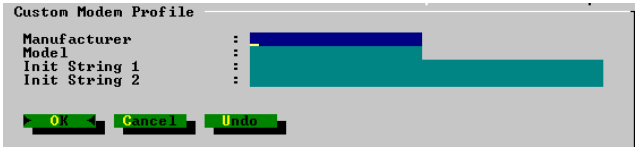
To create or edit a Custom Profile

To create or edit a custom modem profile:

1 From the Advanced Setup main display, select `Port` > `Console Port` > `Modem Profiles` > `Custom`.

- To create a new profile, select `Add`.
- To edit an existing profile, select the profile and then select `Setup`.

2 Configure the parameters on the `Custom Modem Profile` as required.

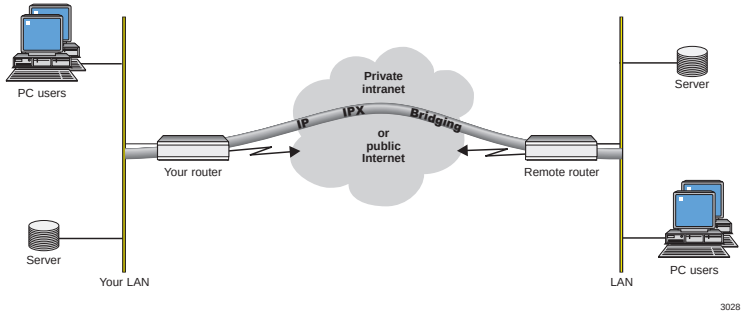


For an explanation initialization string AT commands for supported modems, see Appendix B, “Supported Modems”, p. 329 or refer to modem manufacturer documentation.

Configuring an Internet Tunnel

Internet Tunnels

Internet Tunnels are established to remote networks via the best IP route to an Internet service provider (ISP). This is usually a link directly from this router to your ISP but could also be via a different network device that is accessible from the router.



You can configure a number of Internet Tunnels (see ‘Supported Connections’, p.331). Internet Tunnels are a cost effective solution to transferring data between remote sites; IP and IPX routing and bridging are available over the tunnel. The costs of operation of an Internet Tunnel can be very low when compared to routing via other WAN link types especially when transmitting data over long distances. The throughput of the Internet Tunnel is dependent on the Internet so it can be quite slow at certain times of the day.

Internet Tunnel considerations

The following considerations must be taken into account when setting up an Internet Tunnel:

IP Routing using RIP over the Internet Tunnel

When using IP RIP routing over an Internet Tunnel, a static host route to the remote router via the link from the router to the Internet Service Provider must be established.

If RIP routing is used without the static host route, the router tries to use the Internet Tunnel as the best route to the remote network. The static host route ensures that the Internet Tunnel is established via the route to the ISP and that all the data to the remote router is transferred through the Internet Tunnel.

Site Access Security

Consider access security when using Internet Tunnels. This can be achieved using IP filtering to eliminate unauthorized traffic from the link. A simple example of basic security is given in “Internet Tunnel Example”, p. 135.

Hiding your internal LAN address from the Internet

Dynamic Network Address Translation (NAT) offers the best solution for hiding your internal LAN from the Internet. See “Network Address Translation (NAT)”, p. 192.

Configuration overview

The following shows an overview of how an Internet Tunnel is typically set up in the router to route data between two sites via the public Internet:

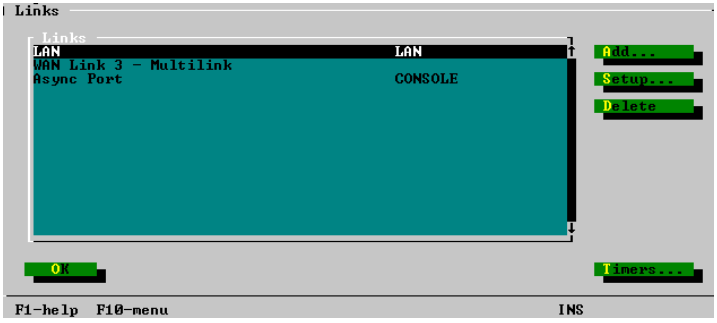
<table>
<tr><td colspan="3">WAN or CSU/DSU port</td></tr>
<tr><td colspan="3">any link from the router to the
Internet Service Provider (ISP)</td></tr>
<tr><td colspan="3">Static IP route
(to the IP address of the remote router over the Internet Tunnel)</td></tr>
<tr><td colspan="3">Internet Tunnel</td></tr>
<tr><td>IP Routing</td><td>IPX Routing</td><td>WAN Bridging</td></tr>
</table>

You must configure the port first. Then configure the link to the ISP for IP routing. The Internet Tunnel can then be configured, followed by the configuring of the routing protocols (IP and Novell IPX) and bridging on top of the tunnel as required.

To configure an Internet Tunnel

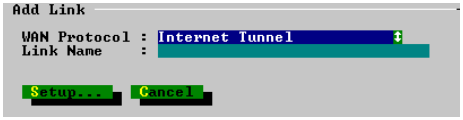
This procedure provides details to add or edit an Internet Tunnel. Before you can establish a tunnel, you must configure a link to your Internet service provider (ISP). See the example procedure “To configure the link to the ISP”, p. 135.

1 From the Advanced Setup main display, select the `Links` option.



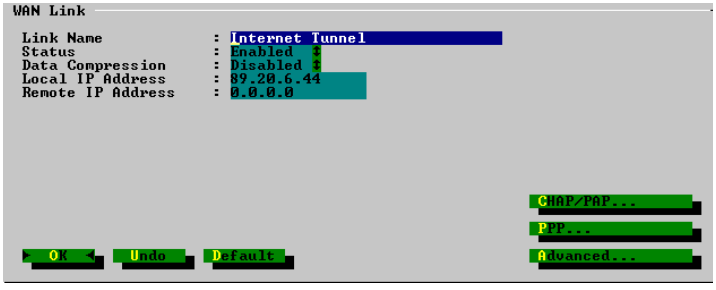
- To configure a new link, select `Add`.
- To edit an existing link, select the link and then select `Setup`. Go to step 3.

2 From the `Add Link` screen, set the `Link Protocol` to `Internet Tunnel`, and enter a name for the link.



To continue, select `Setup`.

3 From the `WAN Link` screen, set the tunnel parameters.



The parameters for the Internet Tunnel that must be configured are:

Parameter	Description
`Data compression`	To enable or disable data compression. It must be enabled in both routers over the Internet Tunnel or compression will not be used.
`Local IP Address`	The IP address for this router used by the remote router over the Internet Tunnel. This can be an IP address assigned to the router, an IP address assigned to the link by the ISP, or the translated IP address if NAT is used. The `Local IP Address` must match the `Remote IP Address` configured on the remote router as seen from the Internet.
`Remote IP Address`	The IP address of the remote router across the Internet Tunnel. The `Remote IP Address` must match the `Local IP Address` configured in the remote router as seen from the Internet. If NAT is used between the router and the Internet, use the translated `Local IP Address` of the remote router.

Configure the other parameters as required.

4 On the `WAN Link` screen, select `Advanced` to set up any advanced link features and parameters.

See “Configuring Advanced Link Features and Parameters”, p. 146 for a description of the advanced link features available.

5 Select the `Protocols` option on the Advanced Setup main display to configure IP routing, IPX routing and bridging.

See Chapter 7 “Configuring IP Routing”, p. 153, Chapter 8 “Configuring Novell IPX Routing”, p. 203 and Chapter 9 “Configuring Bridging Services”, p. 225.

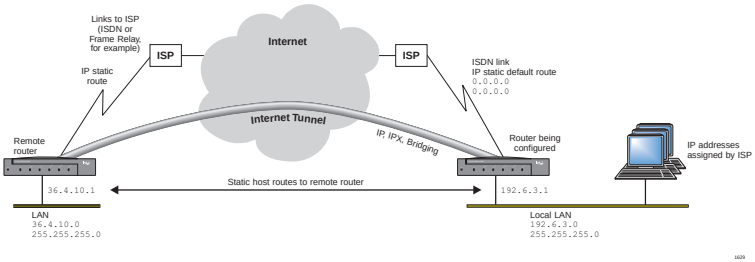
Note If IP RIP is being used over the Tunnel, you must configure a static host route to the IP address of the remote router. See “Configuring IP Static Routes”, p. 200.

Internet Tunnel Example

Example of Configuring a Tunnel for Basic Internet Access

Example

A small company wants to use an Internet Tunnel to route data to another site and provide access to the Internet. The company requires basic security against unauthorized access to the LAN from the Internet. The Express Router can provide the necessary security.

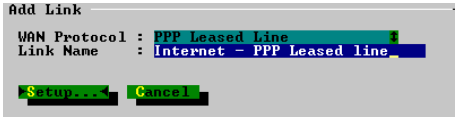


Unless your router uses Network Address Translation (NAT), which translates internal LAN addresses to public IP addresses, only public IP addresses (assigned by your ISP) are used on your LAN. This is a potential security problem. NAT allows a single IP address assigned by your ISP to be used by all the devices on the LAN. This provides some security because your internal LAN addresses will never be seen from the Internet.

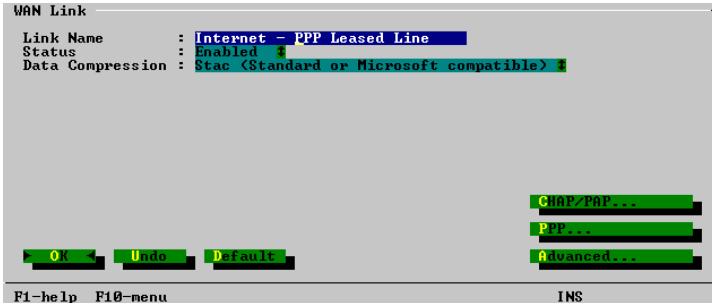
To configure the link to the ISP

Before you configure an Internet Tunnel, you must configure the link to the ISP. This example uses a PPP leased line.

1 From the Advanced Setup main display, select `Links` > `Add` to add the link to the ISP.

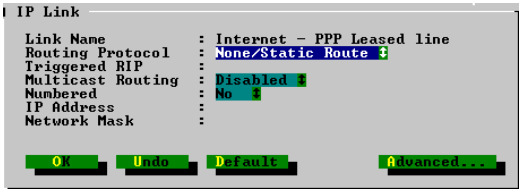


2 Select `Setup` to configure the link.



3 If your ISP requires security using CHAP or PAP, select `CHAP/PAP` on the `WAN Link` screen. See “Configuring Password Protection using CHAP or PAP”, p. 144.

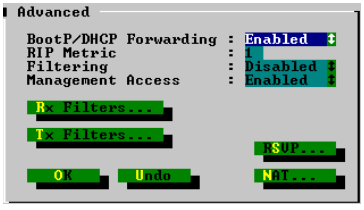
4 From the Advanced Setup main display, select `Protocols` > `IP` to add the link to the ISP.



On the link to the ISP, set the `Routing Protocol` parameter to `None/Static Route`.

The link to the ISP is unnumbered in this example.

5 Select `Advanced` and set the `Filtering` parameter to `Enabled`.



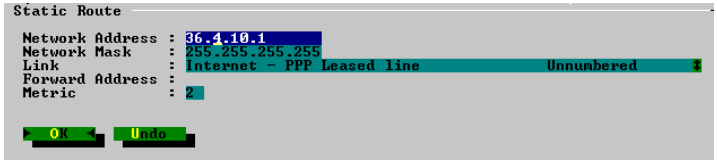
6 Select `Tx Filters` and set the `Default Action` to Pass.

7 From the Advanced screen, select `Rx Filters` to configure the necessary filtering on the link.

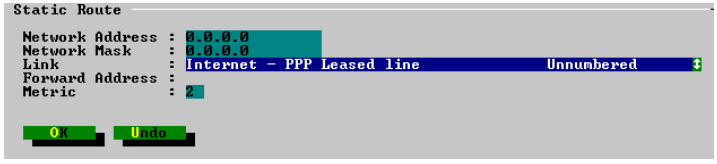
See “Basic Filter Requirements for the Example”, p. 139.

8 Return to the `IP` screen and select `Static Routes`. To configure the static routes, select `Add`.

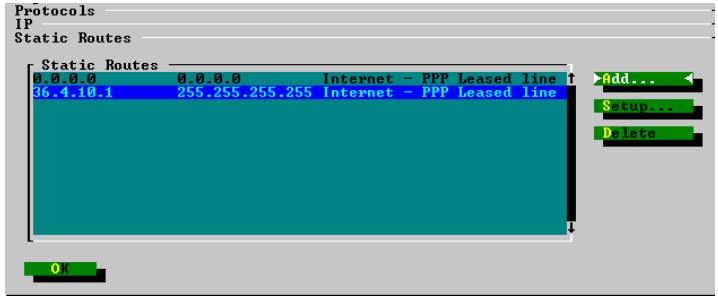
To use IP RIP or Triggered RIP routing on the Internet Tunnel, a static host route to the IP address of the remote router over the Tunnel should be used via the link to the ISP.



Configure a static default route (`Network Address` 0.0.0.0 and `Network Mask` 0.0.0.0) to allow all Internet destinations to be reached via the link.



In this example, two static routes are now defined.



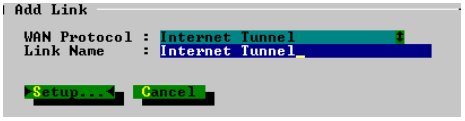
9 Configure the Internet Tunnel as described in the following procedure.

To configure the Internet Tunnel

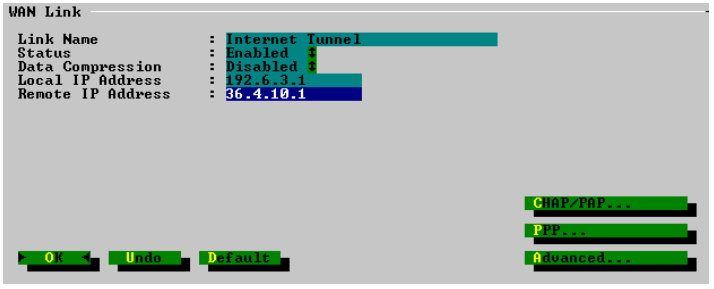
The Internet Tunnel for this example is configured as follows:

1 Enter the `Links` option of Advanced Setup and add an Internet Tunnel to the remote router.

Select `Add` > `Setup` to add the new Internet Tunnel.



Set the tunnel parameters as required.



The `Local IP Address` used for the Internet Tunnel in our example is the IP address of the router being configured (an IP address on the LAN link). The `Remote IP Address` is the IP address of the remote router over the Internet Tunnel.

2 CHAP or PAP can be configured to offer security against unauthorized access to your site from the tunnel, see “Configuring Password Protection using CHAP or PAP”, p. 144.

3 Select the `Protocols` option of Advanced Setup to configure IP routing, IPX routing and bridging on the Tunnel as required by your installation.

See Chapter 7 “Configuring IP Routing”, p. 153, Chapter 8 “Configuring Novell IPX Routing”, p. 203 and Chapter 9 “Configuring Bridging Services”, p. 225.

Basic Filter Requirements for the Example

IP filter configuration using Intel Device View

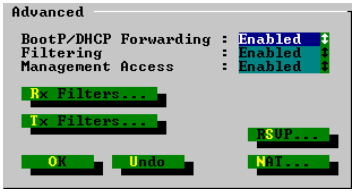
Setting up IP filters can be a complex process. Use the IP Filter Setup program offered from within Intel Device View to configure your IP filters.

Mandatory IP filters required for tunnel example

IP filters must be set up to provide basic security for the Internet tunnel. This example sets up two filters to allow only tunnel traffic to pass over the link to the Internet Service Provider (ISP).

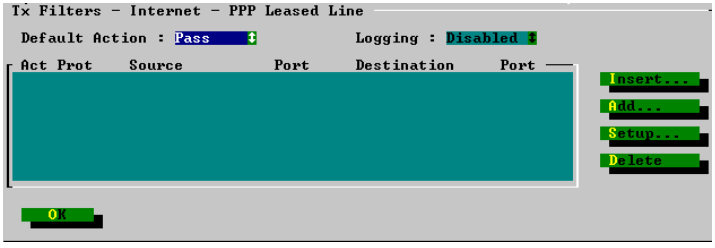
1 Access the `Advanced` screen for the `IP` link to the Internet Service Provider (ISP) from the router.

From the Advanced Setup main screen, select `Protocols` > `IP` > select the ISP link > `Setup` > `Advanced`.



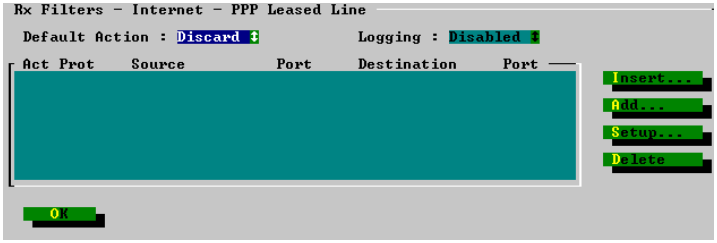
2 Set the `Filtering` parameter to `Enabled`.

3 On the `Advanced` screen, select the `Tx Filters` and set the `Default Action` to `Pass`.



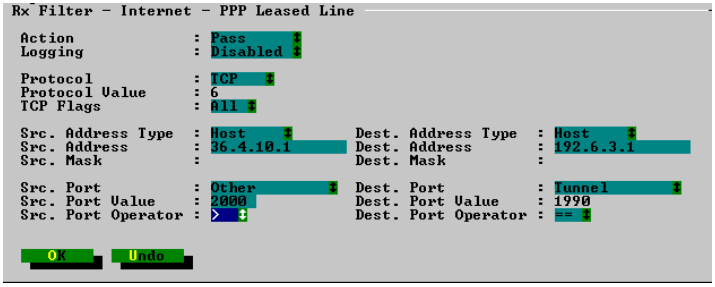
This allows all IP traffic from the router to be transmitted over the link to the ISP.

4 On the Advanced screen, select the Rx Filters and set the Default Action to Discard.



All IP traffic received by the router over the link is discarded unless allowed to pass by specific IP filters.

5 From the Rx Filters screen, select Add to configure a filter to allow incoming traffic to the router to pass to the tunnel port.

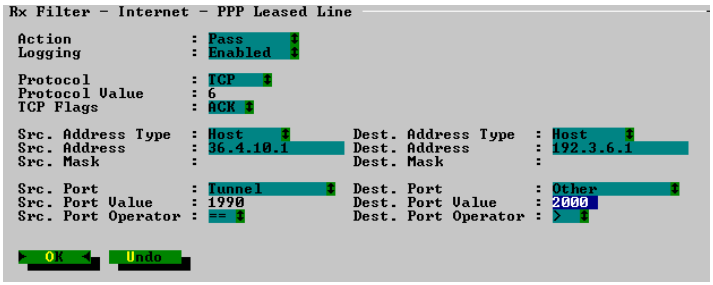


Configure the filter parameters:

Parameter	Set to...
Protocol	TCP
Src. Address Type	Host
Src. Address	IP address assigned to the remote router over the tunnel.
Src. Port	Other
Src. Port Value	2000
Src. Port Operator	>
Dest. Address Type	Host

Parameter	Set to...
Dest. Address	IP address assigned to this router.
Dest. Port	Tunnel
Dest. Port Value	1990
Dest. Port Operator	==

6 From the Rx Filters screen, select Add to configure a filter that allows outgoing traffic from this router to pass to the tunnel port of the remote router.



Configure the filter parameters as follows:

Parameter	Set to...
Protocol	TCP
TCP Flags	ACK
Src. Address Type	Host
Src. Address	IP address assigned to the remote router over the tunnel.
Src. Port	Tunnel
Src. Port Operator	==
Dest. Address Type	Host
Dest. Address	IP address assigned to this router being configured.
Dest. Port	Other

Parameter	Set to...
`Dest. Port Value`	`2000`
`Dest. Port Operator`	`>`

IP filters required for basic WWW access and services

To allow basic World Wide Web (WWW) access and e-mail from the devices on the LAN, the following minimum additional filters are required. These filters are configured from the `Tx Filters` and `Rx Filters` screens for a specific link.

Note Setting up adequate filtering for WWW access can be a complex process and must be tailored to your network environment. The IP Filter Setup program within Intel Device View can help you to set up your required filters.

Note It is up to you to determine which filters are required for your installation, and the filter parameters required to implement them.

- Filters to pass HTTP traffic

  HyperText Transfer Protocol (HTTP) is the main protocol used for WWW communications.

- Filters to pass Domain Name Service (DNS) traffic

  This protocol is used for associating domain names with IP addresses and is used extensively for WWW communications.

- Filters to pass incoming and outgoing mail traffic

  SMTP is used for e-mail transfers between e-mail server and from e-mail clients (for example, user PCs) to e-mail servers. POP3 is used to get mail by e-mail clients from e-mail servers.

  If you have a local e-mail server, incoming and outgoing SMTP access between your local server and the ISP e-mail server is required (2 IP filters).

  If your local clients are connecting directly to the ISP e-mail server incoming POP3 access to the clients from the server and outgoing SMTP access from the client to the e-mail server is required (2 filters).

- Filters to pass FTP traffic, commonly used over the Internet for file transfers.

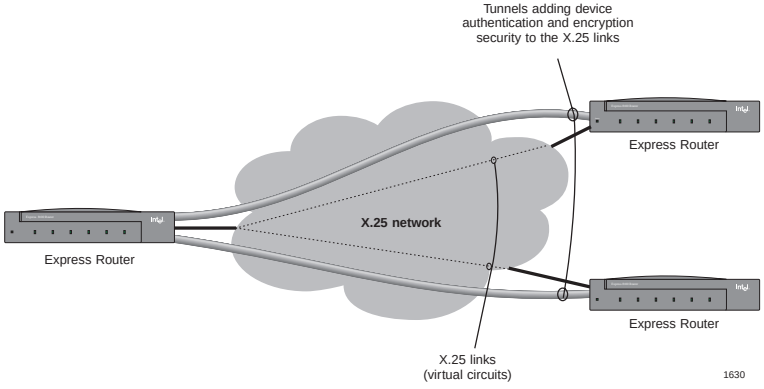
  FTP services should use a proxy server as security is difficult to ensure otherwise.

- Filters to pass NNTP traffic used to get news services from a news server.

Example Use of Internet Tunnels to Offer Data Security over X.25 links

Application of Internet Tunnels for data security over X.25 links

To allow data security over X.25 links, Internet Tunnels can be used on top of them. This offers all the security features supported by PPP (CHAP and PAP) on the X.25 links.



Configuration overview

The following shows an overview of the configuration of an Internet tunnel over an X.25 link.

X.25 port (WAN port configured for X.25)			
X.25 link (PVC or SVC)			additional links
Static IP route to the IP address of the router over the X.25 link			
Internet Tunnel			
IP Routing	IPX Routing	WAN Bridging	

To configure an Internet Tunnel over an X.25 link

To establish a tunnel over an X.25 link, the following steps must be performed.

1. Configure an X25 link as normal. See “Configuring X.25 Services”, p. 118.
2. Configure a single static route on the X.25 link to the IP address of the remote router. See “Configuring IP Static Routes”, p. 200.
3. Configure an Internet Tunnel to the IP address of the remote router. See “To configure an Internet Tunnel”, p. 133.
4. Configure routing and bridging over the Internet Tunnel.

Configuring Password Protection using CHAP or PAP

Peer Authentication using CHAP and PAP

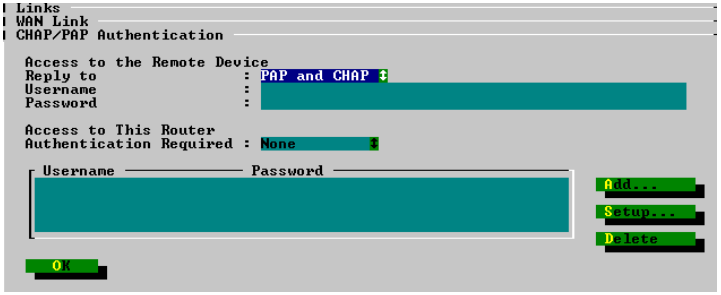
Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) can be configured on PPP links to provide security against unauthorized access. Both protocols use passwords to authenticate peers but CHAP uses password encryption, where PAP uses a simple password.

CHAP and PAP are supported on PPP leased lines, ISDN links, and PPP dial-up modem links on the console port.

For more information about CHAP and PAP, refer the Reference Manual.

To access the CHAP/PAP configuration options for a link

To configure password protection using CHAP or PAP, select the `CHAP/PAP` option on the `WAN Link` setup screen.



To access this feature from the Advanced Setup main display, select `Links` > select the link > `CHAP/PAP`.

To configure CHAP/PAP for access to the remote device

To set up password requirements for access to the remote device over the link, the following parameters must be configured on the CHAP/PAP Authentication options screen.

Parameter	Description
`Reply to`	Determines whether the router will reply to CHAP requests only, PAP requests only or both.
`Own User-name`	The user ID assigned to this router, used in the remote device to verify the correct password is received from the ID. The user name can be up to 47 characters.
`Password`	The CHAP/PAP password required for access to the remote device, associated with the user name. The password defined here must be used by the remote device in response to requests from this router. The password can be up to 47 characters.

To configure CHAP/PAP for access to this router

To set up password protection for access to this router from devices over the link, do the following.

- Select the password access type required for the `Authentication Required` parameter. CHAP offers the best protection and should be used when the device over the link support CHAP
- Select `ADD` to add all device to the list that are allowed to access your LAN via the link. Each device must be assigned a user name and an associated password. The user name and password must correspond to the user name and password set up in the remote router for access to this router. Each can be up to 47 characters.

Configuring Advanced Link Features and Parameters

To access the advanced features and parameters setup for a link

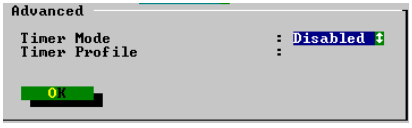
To access the advanced features and parameters screen for a link, select `Advanced` on the `Link` setup screen for the link. From the Advanced Setup main display, select `Links` > select link > `Advanced`.

Advanced screen for PPP leased lines

The following shows the advanced screen for PPP leased line.

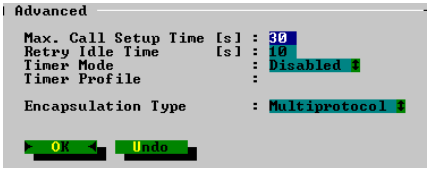
Advanced screen for Frame Relay links

The following shows the advanced screen for a Frame Relay link.



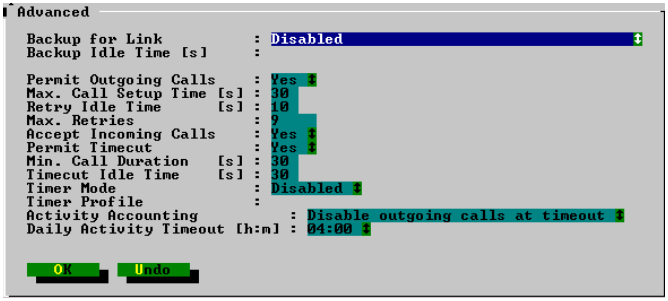
Advanced screen for X.25 PVC links

The following shows the advanced screen for a X.25 PVC link.



Advanced screen for X.25 SVCs, PPP dial-up links and Internet Tunnels

The following shows the advanced screen for the following link types: X.25 SVCs, PPP dial-up modem and Internet Tunnels.



Advanced features

The following describes the advanced features and parameters available depending on the link types.

Backup for another link

The Backup for link parameters defines the link as a backup link. As a backup, the link is then only used if the selected primary link fails.

Parameter	Description
`Backup for Link`	Defines the link or port for which the link being configured is act as a backup.
`Backup Idle Time [s]`	Defines the delay from when the primary (main) link is reestablished until the backup link is disconnected

Call direction controls

These parameters can be used to configure the link for incoming calls only, outgoing calls only or both (default).

Parameter	Description
`Permit Outgoing Calls`	Defines whether the link is to support outgoing calls
`Accept Incoming Calls`	Defines whether incoming calls are to be accepted on this link.

Call setup timing

These parameters control the timing for outgoing call requests from the link to the remote device via the data network. The default values of these parameters should be used in most cases.

Parameter	Description
`Max. Call Setup Time`	The maximum time (in seconds) that is allowed to establish a link with the remote device. On expiry of this time, the router will enter the Retry Idle Time Wait state before attempting to establish the link again.
`Retry Idle Time`	The time (in seconds) from when a call has failed until the router will make another call.
`Max. Retrys`	The maximum number of times that the router will attempt to establish the link. If the number of retries is exceeded, the link will be locked and an error message will be generated in Intel Device View and Local Management. The link can be restarted from Intel Device View or from Local Management.
`Min. Call Duration`	The minimum time (in seconds) from when the link is established until it can be timecut again. If a minimum call charge is made by your service provider, this parameter should be set to the time allowed by the minimum charge.
`Timecut Idle Time`	Defines the time period that a link must be inactive before entering the timecut mode.

Timer profiles

Timer Profiles can either block outgoing calls or all communications over the WAN link at defined time-intervals for each day of the week (see ‘Setting Up Timer Profiles’, p.150). Any of the Timer Profiles defined for the router can be selected for use by the WAN link.

Parameter	Description
`Timer Profiles`	Assigns a Timer Profile to the link. Any of the Timer Profiles defined for the router can be selected for use by the WAN link.
`Timer Mode`	Used to define which traffic from the router to block, outgoing or all, during the time defined by the assigned Timer Profile. If no Timer Profiles are defined, only the `Disable` option is available. If `Block All` is chosen, it is important that the Timer Profile is the same for the router at the other end of the link.

Limiting daily link activity

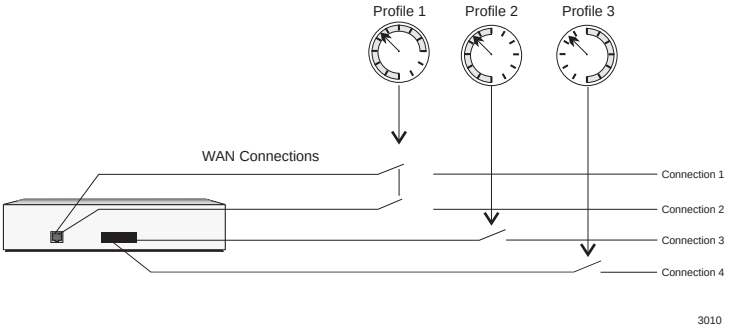
A time limit for use of the link over the course of day can be defined for dial-up links.

Parameter	Description
`Activity Accounting`	Defines what action to take when the time defined by the Daily Activity Timeout has expired. `Disable outgoing calls at timeout` will automatically close and lock the link for outgoing calls (the link can be unlocked from Intel Device View). `Issue warning at timeout` generates an SNMP trap and diagnostic message. `No accounting` will disable the timeout.
`Daily activity Timeout`	Defines the length of time a dial-up link is allowed to be in the up state during the course of a day. Default is 4 hours.

Setting Up Timer Profiles

Timer Profiles

Use Timer Profiles to block out-going calls or all communications over a WAN link between defined time intervals for each day of the week.



The Timer Profiles are configured from Advanced Setup. You can define up to 16 common Timer Profiles for the router. Timer Once defined, the Timer Profiles can be selected for use by the WAN links. A single Timer Profile can be used by a number of WAN links.

To define Timer Profiles

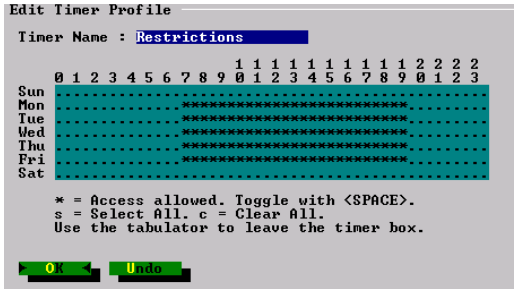
To define Timer Profiles for use by any of the router WAN links:

1 From the Advanced Setup main display, access the `Timers` screen by selecting `Links` > `Timers`.

The `Timers` screen shows the profiles defined for the router.

2 Select `Add` to add new Timer Profiles or `Setup` to edit existing profiles.

3 From the `Edit Timer Profile` screen, define a `Timer Name` and select the times for each weekday when access is disabled or enabled. (See the instructions on how to edit the Timer Profile that follow).



The Timer Profile is a chart with the days of the week along the side and the time-of-day along the top; each cursor position on the chart represents a half hour interval. For each position, access can either be allowed (marked by *) or disabled (marked with .). By default, access is disabled at all times.

4 Once a Timer Profile is defined, it can be used by any of the WAN links.

Editing the Timer Profile

Edit the Timer Profile to suit your own requirements as follows:

To enter the chart area of the Timer Profile

Use the <Tab> key to move from the `Timer Name` parameter to the chart area. A `Timer Name` must be entered to allow the Timer Profile to be selected during configuration of a WAN link.

To move the cursor into position on the Timer Profile

Use the <arrow keys>.

To enable link access at the current cursor position

Use the <space bar> to toggle the time/day position at the cursor from off (.) to on (*).

To disable link access at the current cursor position

Use the <space bar> to toggle the time/day position at the cursor from on (*) to off (.).

To disable (reset) all

Press <`C`> to clear all.

To enable all

Press <S> to select all.

To assign Timer Profiles to WAN links

Timer Profiles are assigned for use by a specific WAN link from `Advanced` option under for `WAN Links` setup.

1. From the Advanced Setup main display, select `Links` > select the link > `Setup` > `Advanced`.
2. Set the `Timer Profile` parameter as required.

7 Configuring IP Routing

Introduction to IP Routing in the Express Router

IP routing (Unicast)

IP routing in the Express Router is used to forward IP traffic addressed to devices on the networks accessible to the router via the LAN and WAN links.

Dynamic Routing using RIP

Routing Information Protocols (RIP-1 and RIP-2) are used to transmit network topology information between routing devices. This enables routers to automatically determine which networks are accessible and the best routes between networks. Routing using RIP is known as dynamic routing as the network will automatically establish itself and dynamically adapts itself to changes.

The correct version of RIP must be selected on a link basis as RIP-2 is not compatible with RIP-1. The router switches between the two RIP versions as necessary.

- RIP-1

  RIP-1 is the original network standard.

- RIP-2

  RIP-2 is a newer version of the RIP standard that offers some improvements over the original RIP including: supernetting, improved RIP update method using multicasts instead of broadcasts, improved subnetting, and routing update authentication.

- Triggered RIP-1 or Triggered RIP-2

  The Routing Information Protocols (RIP-1 and RIP-2) send routing updates at regular 30 second intervals. Triggered RIP sends routing updates only when a network topology change is detected, saving valuable bandwidth on WAN links.

  When used over on-demand or dial-up links, such as X.25 Switched Virtual Circuit (SVCs), conventional RIP may never allow the link to become timecut and the operating costs will be excessive. Triggered RIP only opens on-demand link when a network topology change is detected. This allows you to use dynamic routing with cost-effective use of on-demand links.

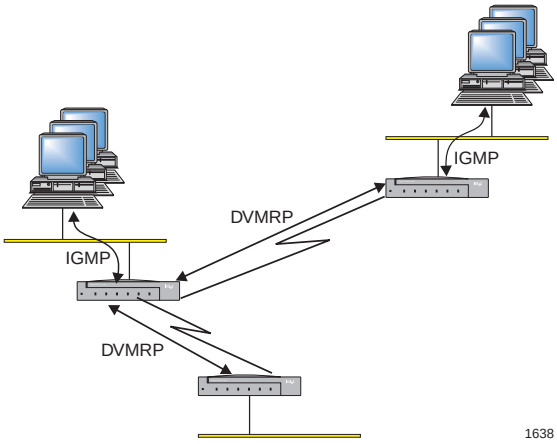
Static routing

Static routes are routes to remote networks that must be manually configured in the router. That is, the route is configured and is not dynamically updated by the router using RIP. By disabling RIP and establishing static routes to the remote networks over a WAN link, routing traffic (RIP updates) can be eliminated from the link. This is useful for slow WAN links for maximizing the available bandwidth for data traffic. Routing using static routes is only really practical for small networks. For larger networks, the router needs to dynamically keep track of network topology changes, and the use of dynamic routing (RIP) is recommended.

IP Multicast Routing

IP Multicast routing

The Express Router supports IP Multicast Routing for multimedia applications that require communications with a number of destinations simultaneously.



Internetworking Group Multicast Protocol (IGMP)

Devices on a LAN use the Internetworking Group Multicast Protocol (IGMP) to communicate IP Multicast destination requirements to routers. The router can use these messages to determine which IP Multicast packets, if any, the LAN should receive.

Distance Vector Multicast Routing Protocol (DVMRP)

IP Multicast Routing over WAN and LAN links use the Distance Vector Multicast Routing Protocol (DVMRP). DVMRP uses routing messages similar to RIP updates to determine the destinations for different IP Multicast packets. Unlike RIP, DVMRP can establish routes to multiple simultaneous destinations for IP Multicast packets. The router therefore only needs to transmit IP Multicasts once which is then simultaneously transmitted on all relevant router links for deliv-

ery to all relevant destinations. Conventional Unicast IP routing would require retransmission of the same information to each individual destination.

Note As with IP RIP, DVMRP sends frequent updates between routers. When used over on-demand or dial-up links, such as X.25 Switched Virtual Circuit (SVC) links, this may never allow the link to become timecut and the operating costs will be excessive.

IP Multicast tunnels

IP Multicast tunnels are used to maintain an IP Multicast network through routers that do not support IP Multicasts using the Distance Vector Multicast Routing Protocol (DVMRP), see “Configuring IP Multicast Tunnels”, p. 162.

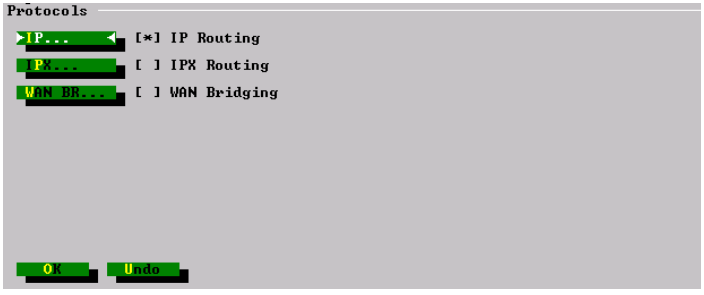
Configuring IP Routing on LAN and WAN Links

To configure IP routing on the LAN and WAN links

To configure IP routing on the LAN and WAN links:

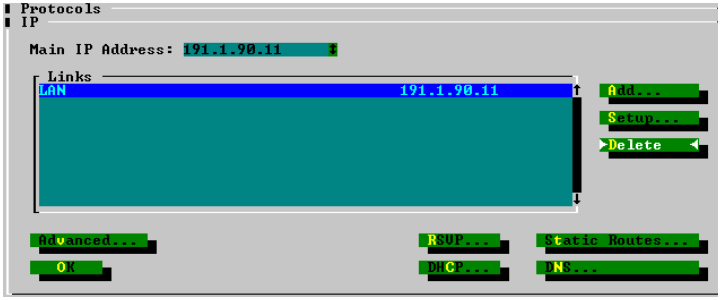
Note All the configuration parameters in Advanced Setup are described in on-line help. To access the help for a parameter, click on the parameter and press the `F1 Help` key.

1 Enter the `Protocols` option of Advanced Setup.



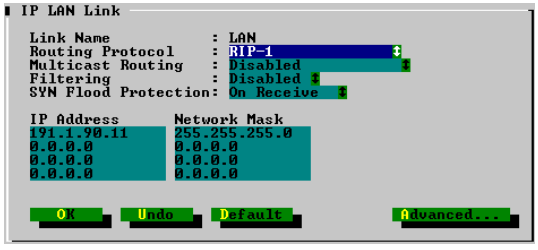
IP routing services are enabled by default. If you need to enable or disable IP routing, click the `IP Routing` check box on the `Protocols` screen. IP routing is enabled if the check box is marked with an asterisk `[*]` and disabled if the check box is empty `[ ]`.

2 Select `IP` on the `Protocols` screen.



3 Use `Add` to add IP routing to a LAN or WAN link not listed or `Setup` to edit the IP routing configuration for an existing link.

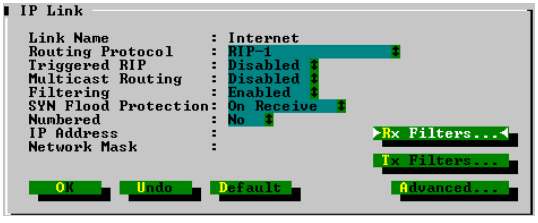
- The IP setup screen for the LAN link is as shown below.



The `Routing Protocol` parameter must be set to the correct version of RIP in use on your LAN. Four different IP networks are allowed on an Ethernet LAN and the router can communicate between all four IP networks.

`Multicast Routing` should only be enabled if IP Multicasts are required by applications on the LAN or the IP Multicast topology includes the LAN.

- The IP setup screen for WAN links is shown below.



The WAN link parameters on the `IP Link` screen that must be configured are given in the following table.

Parameter	Description
`Routing Protocol`	Defines the routing protocol for use over the link (RIP-1 or RIP-2) or if static routing is to be used. The routing protocol (RIP-1 or RIP-2) or static routing must be the same in both the routers over the link. If `None/Static` is selected, static routes must be established to the remote networks. See “Configuring IP Static Routes”, p. 200
`Triggered RIP`	This parameter enables the use of Triggered RIP over the link to reduce the bandwidth overheads of RIP routing. If the link is an on-demand type such as X.25 Switched Virtual Circuit (SVC) link, the use of `Triggered RIP` is recommended. Triggered RIP must be enabled in both routers over the link or IP routing over the link will not function correctly.
`Multicast Routing`	Multicast Routing should only be enabled if IP Multicasts are required on the link and should only be enabled if the router over the link supports IP Multicast routing using the Distance Vector Multicast Routing Protocol (DVMRP) and IGMP for the LAN.
`Filtering`	Enable Filtering if IP filtering is required on the link. See “IP Filters and Firewall Protection”, p. 167.
`Syn Flood Protection`	Enable Syn Flood Protection on either receive or transmit traffic. See “SYN Flood Protection”, p. 172 for details.
`Numbered`	A numbered link (where an IP address is assigned to the link in the router) is sometimes required for a link to an ISP or third party router. A unique `IP Address` and `Network Mask` for the link must be entered when using a numbered link.

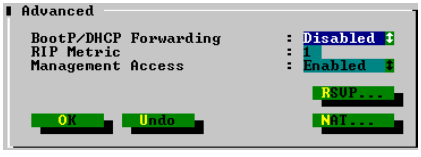
Parameter	Description
`Dynamic IP Address`	Some Internet Service Providers (ISPs) dynamically assign an IP address to devices on call link. Select `Dynamic IP Address` if required by an ISP link. Contact your ISP if you are unsure whether dynamic IP addressing is required.

The other parameters can be configured to your requirements.

4 Select `Advanced` on the Link screen and set up any advanced link parameters and features required.

An example of the `Advanced` screen for a LAN link is shown below.

An example of the `Advanced` screen for a WAN link is shown below.



Set the parameters on the Advanced screen are as follows:

Parameter	Description
BootP / DHCP Forwarding	BootP / DHCP Forwarding must be enabled if devices are being booted via the router or if IP addresses are dynamically being requested from a DHCP server over the WAN link or on the LAN. This parameter should also be enabled if managing remote devices over the link from Intel Device View on your LAN. This parameter need not be enabled if the boot server or DHCP server is on the LAN, BootP and DHCP responses are always forwarded.
ProxyARP	ProxyARP can be enabled to answer ARP requests from devices on the LAN that do not use the router as the primary gateway and are not able to determine the MAC address of a remote host in any other way. If disabled the router does not respond to ARP requests on behalf of the remote hosts.
RIP Metric	RIP metrics are used to determine if a destination is reachable and the priority for use of a link when multiple routes to a destination network are available.
Authentication Type and Key	The Authentication parameters are only available if RIP-2 was selected for the Routing Protocol and allow simple password protection of RIP updates using an Authentication Key (password).
DVMRP Metric	This parameter is only available if Multicast Routing is enabled for the link. Like RIP, DVMRP uses metrics to determine if a destination is reachable and the priority for use of a link when multiple routes to a destination network are available.

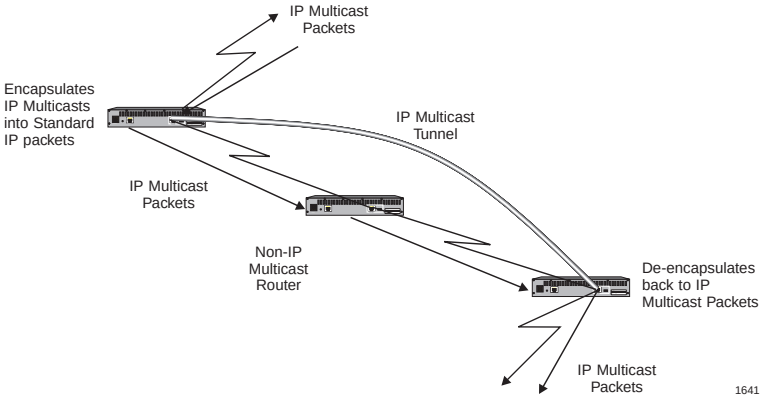
Parameter	Description
`TTL Threshold`	This parameter is only available if Multicast Routing is enabled for the link. This parameter can be used to limit the range of IP Multicast packets. IP Multicast packets with a Time-To-Live of less than the value specified by this parameter will not be allowed over the link.
`Manage-ment Access`	Enables or disables management access to the router via this link. When disabled, all TFTP, SNMP, Telnet, or BootP packets received on this link are discarded.

- Setting up IP filters (accessed by selecting `Rx Filters` and `Tx Filters`) is described in “To Configure Firewall Protection and IP Filters and on LAN and WAN Links”, p. 174.
- Setting up Network Address Translation (`NAT`) is described in “Network Address Translation (NAT)”, p. 192.
- Setting up the Resource ReSerVation Protocol (RSVP) to reserve link bandwidth for applications which require guaranteed data delivery is described in “Configuring Bandwidth Reservation using RSVP”, p. 164.

Configuring IP Multicast Tunnels

IP Multicast Tunnels

IP Multicast Tunnels must be established to maintain the IP Multicast network topology via routers that do not support IP Multicasts using the Distance Vector Multicast Routing Protocol (DVMRP). Otherwise, the non-IP Multicast routers will discard IP Multicasts.



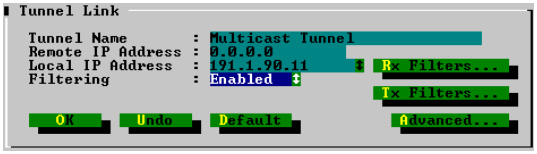
The IP Multicast Tunnel must be set up in both the routers over the tunnel. IP Multicast packets traversing the tunnel are encapsulated into conventional IP packets (Unicast). These packets are routed as normal IP packets via the non-IP Multicast routers. When they reach the other end of the IP Multicasts Tunnel, the packets are de-encapsulated into the original IP Multicast packets for transmission through the rest of the IP Multicast network.

To configure IP Multicast Tunnels

Follow this procedure to configure IP Multicast Tunnels for the router.

1. Enter the `Protocols` option of Advanced Setup.
2. Select `IP` on the `Protocols` screen.
   - To add a new IP Multicast Tunnel, select `Add`> `Multicast Tunnel`>`Setup`.
   - To edit an existing IP Multicast Tunnel, highlight the tunnel from the list and select `Setup`.

3 Configure the Multicast Tunnel parameters.

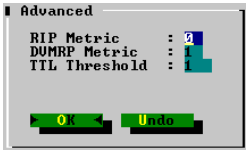


The following parameters are available.

Parameter	Description
`Tunnel Name`	Descriptive name, up to 30 characters.
`Remote IP Address`	The IP address of the remote router over the Multicast Tunnel which supports the Distance Vector Multicast Routing Protocol (DVMRP) and Multicast Tunnels.
`Local IP Address`	The IP address for the router being configured as seen by the remote router over the Multicast Tunnel. This can be an IP address assigned to the LAN of the router or an IP address assigned to a WAN link if using a numbered link.
`Filtering`	Enable `Filtering` if IP filtering is required on the link.

Setting up IP filters (accessed by selecting `Rx Filters` and `Tx Filters`) is described in “To Configure Firewall Protection and IP Filters and on LAN and WAN Links”, p. 174.

4 Select `Advanced` on the `Tunnel Link` screen and set up any advanced link parameters and features required.



The following parameters are available on the Advanced screen for an IP Multicast Tunnel.

Parameter	Description
RIP Metric	Used to identify the shortest or best route to a destination. The some of RIP metrics for a route to a destination must not exceed 15.
DVMRP Metric	Like RIP, DVMRP uses metrics to determine if a destination is reachable and the priority for use of a link when multiple routes to a destination network are available.
TTL Threshold	This parameter can be used to limit the range of IP Multicast packets. IP Multicast packets with a Time-To-Live of less than the value specified by this parameter will not be allowed over the Multicast Tunnel.

Configuring Bandwidth Reservation using RSVP

Resource Reservation Protocol (RSVP)

The Resource Reservation Protocol (RSVP) is used to reserve bandwidth along the route between remote devices for applications which require a guaranteed bandwidth for satisfactory operation. A typical example of such an application is video conferencing.

To configure RSVP

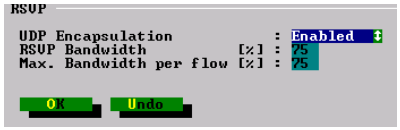
The Resource Reservation Protocol (RSVP) is configured by default for the router. RSVP does not have any network overheads and does not take any router resources if it is not used. However, some advanced settings for RSVP are available.

Note Under normal circumstances, the default values of the parameters on the RSVP screens should be used.

To configure RSVP for each IP link

The RSVP configuration screen for a link is accessed from the `Advanced` screen for an IP link setup.

- From the `IP` screen, highlight the link and select `Setup`>`Advanced`>`RSVP`.



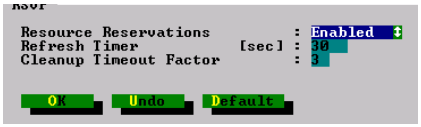
- Configure the parameters according to the following.

Parameter	Description
`UDP Encapsulation`	This enables or disables UDP encapsulation of RSVP message packets transmitted. RSVP messages are usually transmitted using an IP RSVP packet type, which may not accepted by all devices on your network. If you have devices on your network that do not accept IP RSVP packets, this parameter must be enabled. When enabled, messages are transmitted in both IP RSVP and UDP format.This is the default setting and is recommended for most applications.
`RSVP Bandwidth`	Defines how much of the link bandwidth can be reserved by applications using RSVP. If the link receives a reservation request that is greater than the amount defined here, the request will be rejected.
`Max. Bandwidth per flow`	Defines how much of the available link bandwidth can be reserved for any one application using RSVP. This value must be less than or equal to the RSVP bandwidth. If the link receives a reservation request that is greater than the amount defined here, the request will be rejected.

To Configure RSVP for the Router

The RSVP configuration screen for the router is accessed by selecting the RSVP option from the IP screen.

- From the Advanced Setup main display, select Protocols> IP>RSVP.



- Configure the RSVP parameters as required.

Parameter	Description
Resource Reserva-tions	Enables or disables bandwidth reservation using RSVP for the router.
Refresh Timer	Once the reservation has been established, the routers on either end of the link exchange refresh messages (Reserve and Path messages) to maintain the reservation and path. This parameter defines the time interval between messages.
Cleanup timeout factor	Defines the number of refresh messages that can be missed before the router clears a reservation

IP Filters and Firewall Protection

IP Filters and Firewall Protection

A firewall restricts access between networks, both private and public such as the Internet. A firewall filters all network packets to determine whether to send them to their destination. The Express Router implements comprehensive IP packet filtering to restrict access between networks and to limit unnecessary traffic to save on bandwidth. These filters provide the basis for setting up a firewall. The router offers two types of filters, static and stateful.

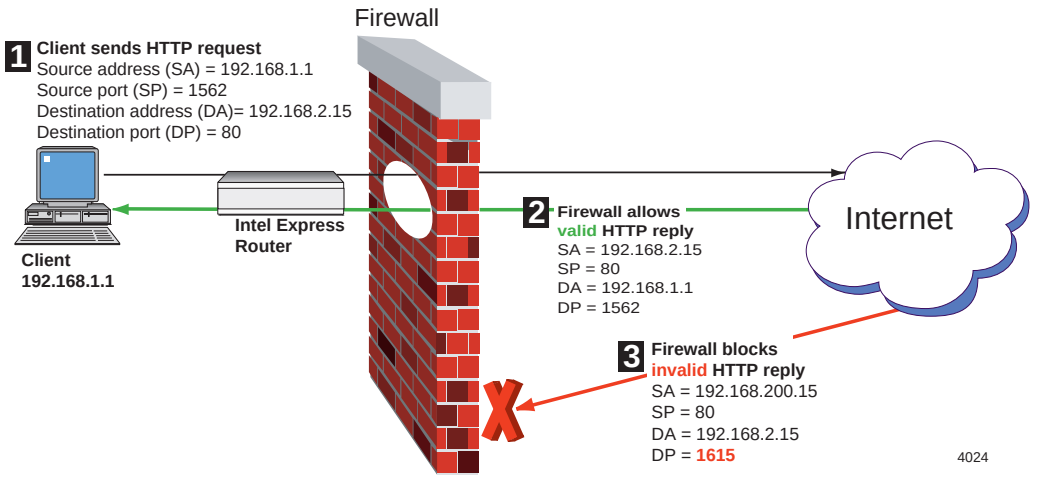
Note A good understanding of IP is required before effective filtering can be set up in the router. Filters must be defined as strictly as possible to eliminate unauthorized access to services, hosts and networks.

Static Filters

Static filters can discard or pass incoming and outgoing packets on a link. The router checks each packet as it arrives to see it if meets the criteria set by the filter. If so, the packet will be discarded or passed depending on the action you define. These filters are called static because they do not change state. They are basically always active. The router does not monitor the state of a transaction, that is, it does not remember when a packet is passed or the source and destination of the packet.

Stateful Filters

Stateful filters are time-limited dynamic packet filters for TCP, UDP, and ICMP, based on the principles of stateful inspection. Stateful inspection monitors state information of a connection by recording source and destination IP addresses and port numbers of inbound and outbound traffic. A stateful filter uses this information to determine whether to allow a packet to pass through the firewall. For a response packet to pass the firewall, the inbound packet has to be from the host and port that the outbound packet was sent to, and it has to be directed to the host and port that sent the outbound packet.



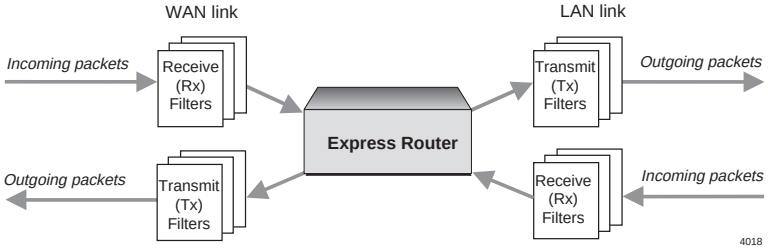
The process is shown in the illustration above. When a request is sent from a source to a destination, the stateful filter virtually opens a hole in the firewall and the packet is allowed to pass. Only a response that matches the state information of the request packet will be allowed back through the firewall. Packets which do not match the state information are discarded. When a valid response is received, it is allowed to pass by the stateful filter. The filter then deactivates thus closing the hole in the firewall.

Stateful filters are also time-limited. If a correct response is not received within a certain amount of time, the filter closes and discards subsequent response packets.

Stateful filters offer much higher security than static filters. For example, using static filters in the illustration, you would need to permanently allow inbound replies from all external ports (assuming users can visit any site on the Internet). This would allow attackers to penetrate the firewall by making inbound or request packets look like replies.

Filter direction - transmit or receive

You define IP filters on a link basis for each interface. Filters can discard or pass both received and transmitted packets on a link. The router is the reference point that determines the filter direction, receive or transmit, as illustrated in the diagram.



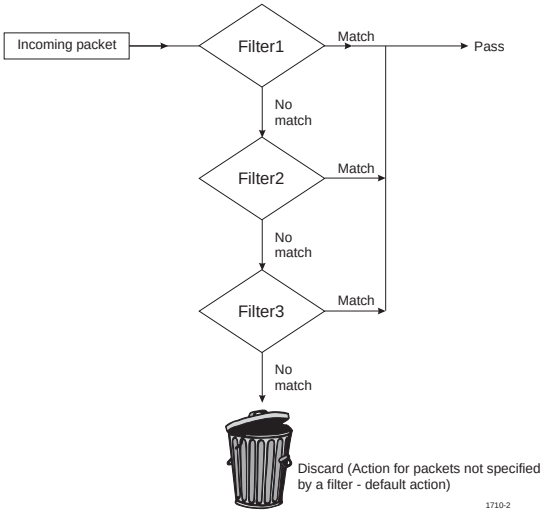
For example, if you are configuring filters on your LAN link, use receive filters to filter packets incoming from your LAN; to filter packets from the WAN to the LAN, use transmit filters.

Packet processing by filters and filter order

The order of the filters you define is important. The order will depend on your filtering requirements. When the router encounters IP packets, it compares the packets to the filters in the order defined in the list. If a packet meets the criteria of a filter, it is either passed or discarded, according to the action defined. If a packet matches more than one filter, it will be processed by the first matching filter only.

Note The exception to this rule occurs when you have configured both static and stateful filters. Static filters take priority over stateful filters. The router searches the filter list and compares packets first to static filters followed by stateful filters. It is recommended that you place static filters before stateful filters. See “Common practises and recommendations”, p. 178 for details.

The following diagram shows how the router processes packets by the IP filters when a number of discard filters are defined. When configuring filters, you must also select a default action (action performed on packets not specified by filters).



With the default filter action for a link set to pass, all incoming (for Rx filters) or outgoing (for Tx filters) IP packets on the link will be allowed to pass unless otherwise discarded by a filter.

Logging filtered packets

The router can be set up to log filtered packets. This is a useful tool for troubleshooting the filters to ensure that they are operating as expected, and for detecting hits on the filters in case of an attack from an unauthorized source.

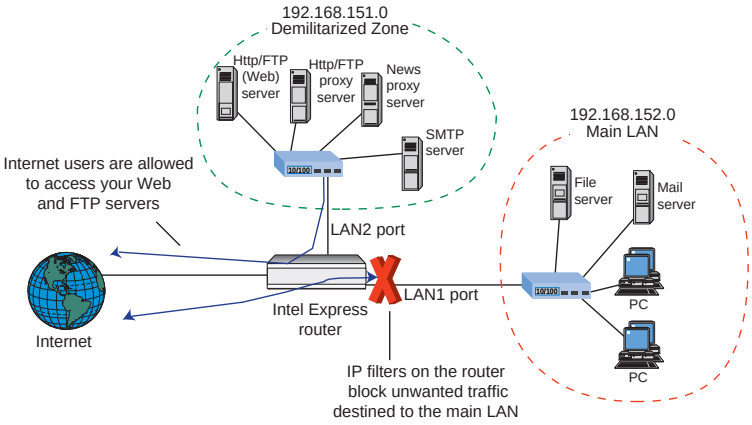
Note Logging reduces the performance of the router slightly. You should only enable it when required, such as for troubleshooting or when an attack is suspected.

Packets are recorded in the system log, which you can view from Intel Device View or Local Management.

DMZ solution using the second LAN port

On an Express Router that has two LAN ports, you can set up a DMZ (demilitarized zone) on the LAN2 port to protect your private network from the public network (Internet). A DMZ is a network added between a protected network and a public (external) network that provides an additional layer of security. Use the DMZ to give access to services required from the Internet and your private network on

LAN1. These services are typically Web servers, FTP servers, News servers, or SMTP servers. IP filters on the LAN1 prevent access to your private network from the Internet.



You can set up a DMZ using static and stateful filters. For an example using stateful filters, see “Setting Up a DMZ Firewall Using Two LAN Ports”, p. 187. For a detailed explanation using static filters search for a DMZ Application Note on the Intel Customer Support Web site at http://support.intel.com.

Features of Stateful Filters

Port-to-application Mapping

Port-to-application Mapping

Port-to-application mapping is available for the TCP protocols HTTP and FTP. This allows you to use non-standard port numbers for these services when using stateful pass filters. For example, the typical port number for FTP is 21. In some cases, you may want to assign a different port number to this service on your network. By design, a firewall using stateful pass filters identifies FTP by port 21.Therefore in order for the stateful pass filter to work correctly, you must direct, or map, the FTP application to this port. To configure port-to-application mapping, see “To configure IP filtering on the LAN and WAN links”, p. 174.

SYN Flood Protection

SYN Flood Protection

SYN Flood Protection is a method to combat against SYN Flood attacks on your network. SYN flood attacks can be extremely damaging to TCP services such as WWW, FTP, and e-mail.

What is a TCP Syn Flood Attack

A TCP connection is initiated when a source host, identified by its IP address, issues a SYN request to a destination, such as a Web server. Under normal circumstances, the destination will send a SYN ACK back to the source host and await ACK back from the source. While the destination waits for the response, it holds the connection in a connection queue along with other pending connections. When the destination receives the ACK from the source the connection is established.

In a TCP SYN flood attack, the source host generates a number of requests to a destination using spoofed or random IP addresses. When the destination sends a SYN ACK back to the random IP address, the source is unreachable and the destination never receives an ACK in return. The connection remains in the queue until it times out, which is about one minute. The connection queue is of finite size. If the source sends requests at a rapid rate, it is possible to fill the connection queue. This can result in TCP services, such as WWW and e-mail, being denied to legitimate users.

How TCP SYN Flood Protection Works

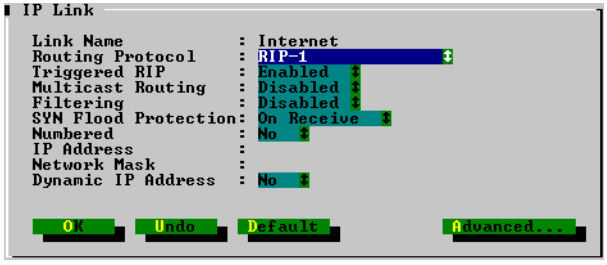
Protection against SYN flood attacks is done with the help of the firewall and stateful filters. Acting on behalf of the destination, the firewall intercepts a SYN request from a source. The firewall returns a SYN ACK to the source host. If the firewall receives an ACK from the source, it forwards a SYN request to the destination host. When the firewall receives a SYN ACK back from the destination, it returns an ACK and the connection is established.At any time during the process, if the firewall does not receive an ACK from the source or destination within a certain amount of time, it terminates the connection.

To configure SYN Flood Protection

SYN Flood Protection is active only when a firewall is present using stateful filters. You configure SYN Flood Protection on a connection or link basis for either packets received on the link (inbound to the router) or packets transmitted on the link (outbound from the router). The typical set up is on receive packets, which is the default setting. To configure SYN Flood Protection:

1 Access the `IP Link` screen for the link.

This is done from the Advanced Setup main display by selecting `Protocols` >`IP` > select `link` > `Setup`.



2 Set the `SYN Flood Protection` parameter on the IP Link screen.

- Set it to On Receive to protect from SYN attacks inbound to the router.

  This setting would be typical when configuring a WAN connection to the Internet.

- Set it to On Transmit to protect from SYN attacks outbound from the router.

  This setting is typical when configuring a LAN connection for protection against SYN attacks from the Internet.

To Configure Firewall Protection and IP Filters and on LAN and WAN Links

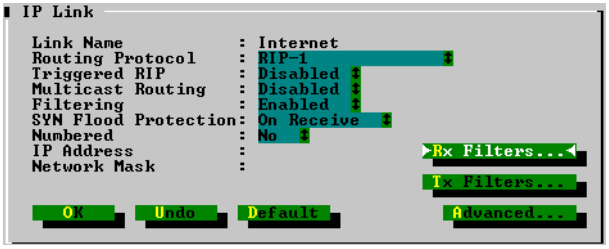
To configure IP filtering on the LAN and WAN links

Follow this procedure to configure IP filtering on the LAN and WAN links:

Note Before you begin adding filters, see “Common practises and recommendations”, p. 178 for help in setting up a firewall.

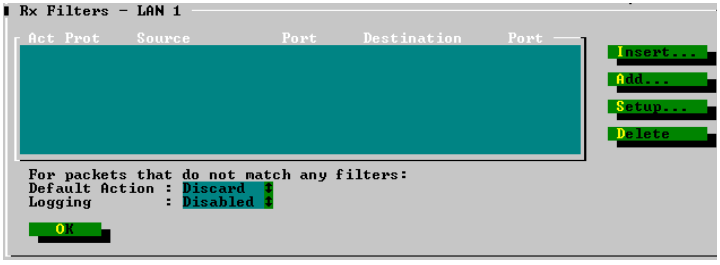
1 Access the `IP Link` setup screen for the IP link you want to configure.

This is done from the Advanced Setup main display by selecting `Protocols` >`IP` > select `link` > `Setup`.



2 Set the `Filtering` parameter to `Enabled`.

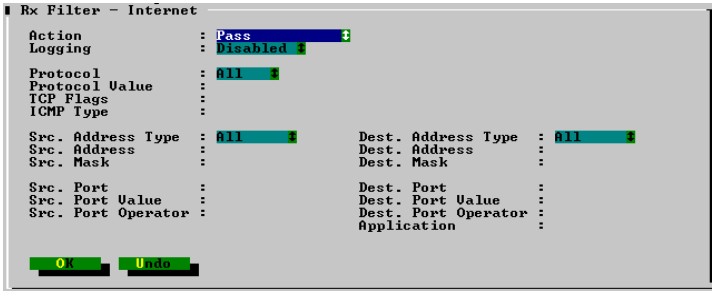
3 To configure receive filters, select `Rx Filters`. Receive filters pass or discard incoming traffic from the link.



- Set the `Default Action` to Discard to discard all data from the link which is not allowed to pass by specific filters. Set this parameter to `Pass` to pass all packets except packets discarded by specific filters.

- The `Logging` parameter should normally be set to `Disabled` to minimize router processing overheads. However, set this parameter to `Enabled` to troubleshoot the filters. When enabled, the details of all packets discarded by the default action for the filters will be logged in the System Log for the router.

4 Use `Add` to add a new filter after the selected filter, `Insert` to add a new filter before the selected filter, or `Setup` to edit the selected filter.



Note Packets will be filtered using the first filter in the list which matches the packet.

Define the filter criteria as required. See “Filter criteria” that follows.

5 Set the action for the filter.

Setting	Description
`Discard`	Defines a static filter to block packets that match the filter criteria from continuing to the destination. This setting is typical if the action for traffic not filtered is set to pass.
`Pass`	Defines a static filter that allows packets that match the criteria to pass to the destination. This setting is typical if the action for traffic not filtered is set to discard.
`Stateful Pass`	Defines a stateful filter that allows all packets which meet the criteria to pass through the firewall.

6 Define the filter criteria as required. See “Filter criteria” that follows.

7 Select `Tx Filters` from the `Advanced` screen for the IP link to define transmit filters. Transmit filters pass or discard outgoing traffic on the link.

The procedure for Setting up receive (Rx) and transmit (Tx) filters is the same.

Filter criteria

Each filter in the Express Router can be set up to discard, pass or stateful pass IP packets based on the following criteria:

IP Protocol

You can filter on all IP protocols. Static filters (Discard or Pass) can be set up for all IP Protocols. Stateful pass filtering is available for TCP, ICMP, and UDP protocols. Depending on the protocol chosen, a filter can process packets based on:

Parameter	Description
`Protocol`	Selects the IP protocol on which to filter. You can filter on all protocols by selecting All or a single protocol. The most common protocols, such as TCP, UDP and ICMP are listed. To select another protocol, set the parameter to Other and enter the appropriate number in the Protocol Value field.
`Protocol Value`	This is the standard protocol port number as listed by RFC 1700.

Parameter	Description
TCP Flags	TCP flags distinguish between requests to establish a TCP connection (ACK not set) and subsequent communications on an established TCP connection (ACK set). Since TCP flags are typically not set for the first session request and set in all following session communications, filtering of the TCP flag can prevent sessions being established on internal devices from remote devices, and vice versa. To allow TCP connection requests and subsequent communications, set the parameter to TCP flag to All. To prevent external TCP connections from being established, set the TCP flag to ACK.
ICMP type	You can filter ICMP messages based on the ICMP header types available. ICMP delivers IP status and control messages, which is used in functions such as ping. ICMP messages are useful when troubleshooting. Each ICMP message is defined by message type header. Select the type from the list.

Source (Src.) Address

To filter packets entering the router via the link from a specific host or network.

Source (Src.) Port

To filter packets originating from a single port (for example FTP data, Telnet, SMTP), or from a range of ports or all ports.

Port Operator	Function
== default value	Only packets from the specified TCP/UDP Src. Port or Src. Port Value are filtered
!=	All TCP/UDP ports except the specified Src. Port or Src. Port Value are filtered. (Not available for stateful pass filters.)

Port Operator	Function
>	All TCP/UDP port numbers above (but not including) the specified `Src. Port` or `Src. Port Value` are filtered. (Not available for stateful pass filters.)
<	All TCP/UDP port numbers below (but not including) the specified `Src. Port` or `Src. Port Value` are filtered. (Not available for stateful pass filters.)

Destination (`Dest.`) Address

A filter can process packets addressed to a host address or a network address.

Destination (`Dest.`) Port

A filter can process packets addressed to a single port (for example FTP control, TFTP, SNMP), or a range of ports or all ports. See "Source (`Src.`) Port" above.

Port to Application Mapping (`Application`)

This parameter directs TCP services FTP or HTTP to non-standard port numbers. See "Port-to-application Mapping", p. 171 for details. Only stateful pass filters have this option. Choose FTP or HTTP as required. If you are using standard port numbers, set this parameter to Use Port.

Common practises and recommendations

Here are some common practices and recommendations you should follow when configuring a firewall using IP filters in the Express Router. These will help increase the integrity of your firewall and make it easier to troubleshoot any problems that might occur.

Default filter action on all links

Set the default action for traffic not specified by a filter to discard on all links. Then for each specific link, add the necessary filters for outbound and inbound services, such as HTTP and FTP.

Receive and Transmit filters on private LAN

When you are setting up a DMZ on the second LAN port of the router, you want to create filters on your private LAN to pass only inbound and outbound traffic to and from the DMZ.

- Configure receive (Rx) filters to pass traffic to servers on the DMZ.
- Configure transmit (Tx) filters to pass traffic from servers on the DMZ.

Receive and Transmit filters on Internet connection

Configure receive (Rx) filters to pass public services (typically SMTP, HTTP, and FTP) to servers on the DMZ. Configure transmit (Tx) filters to pass all traffic or, to restrict access, configure pass filters for traffic you want to allow and discard all other traffic. Keep in mind that security is increased by using both Rx and Tx filters. However, with stateful filters, you only need to configure Tx filters for outgoing services and Rx filters for incoming services. An example of this is to configure Tx filters to allow outgoing DNS, HTTP FTP and SMTP services and only a single Rx filters to allow incoming SMTP.

Receive and Transmit filters on the DMZ (LAN2) interface

Since filtering is set on the Internet connection and private LAN, you can disable filtering on the DMZ interface. You can, however, increase security using receive and transmit filters on your DMZ. To get this additional security, add pass (static) and stateful filters for services to and from the DMZ (typically DNS, SMTP, HTTP, and FTP) as required.

Order of static and stateful filters

Static filters take priority over stateful pass filters. This means that the router acts on all static filters (pass or discard) before stateful pass filters no matter the order in the filter list for a link. For example, you have configured two filters in the following order: 1) a stateful filter to pass UDP packets from a specific source and 2) a static filter to discard all UDP packets. Because static filters have priority, all UDP packets will be discarded and filter 1 is ignored.

To avoid this situation and help the organization of your filters, place all static filters ahead of stateful pass filters in the filter list.

Logging filters

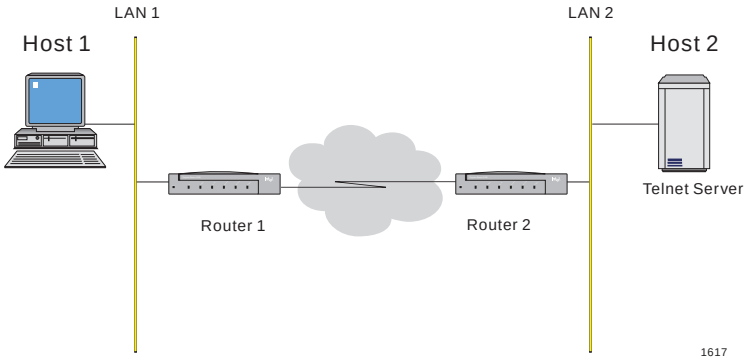
Under normal circumstances, you should only activate logging for discard filters on your Internet connection (see “Logging filtered packets”, p. 170). If troubleshooting is necessary, enable logging for receive and transmit filters on all links.

Static IP Filter Examples

Filtering Telnet

Filter requirement

Host 1 on LAN 1 must have Telnet access to remote Host 2 on LAN 2 (but Host 2 must not be able to establish a Telnet session onto Host 1).



IP traffic

The TCP/IP traffic to establish a Telnet session from Host 1 to Host 2 is:

Direction	Flags	Source Add.	Source Port	Dest.	Dest. Port	Comments
1 > 2	ACK = 0	Host 1	X	Host 2	23	Telnet request from Host 1 to Host 2.
2 > 1	ACK = 1	Host 2	23	Host 1	X	Telnet response from Host 2 to Host 1—connect to Port X (where X > 1023).
1 > 2	ACK = 1	Host 1	X	Host 2	23	Telnet command.

Filters required

Filters are required in Express Router 1 to protect LAN 1 from unauthorized access and so that only Host 1 is allowed to establish a Telnet session onto Host 2.

The filters required are as follows:

Rx Filter on the WAN Link of Express Router 1

This filter only allows TCP access from the WAN link from Host 2 to Host 1, with the ACK flag set (session established), a Telnet server source port and a destination port of greater than 1023 (unassigned ports used by the Telnet client).

Parameter	Setting
Default Filter Action (on Advanced screen)	Discard
Action (Filter action)	Pass
Protocol	TCP
TCP Flags	ACK
Src. Address Type	Host
Src. Address	Host 2’s IP address
Src. Port	Telnet
Src. Port Operator	==
Dest. Address Type	Host
Dest. Address	Host 1’s IP address
Dest. Port	Other
Dest. Port Value	1023
Dest. Port Operator	>

Tx Filter on the WAN link of Express Router 2

This filter only allows TCP access to the WAN link from Host 1 to Host 2, with a source port of greater than 1023 (unassigned ports used by Telnet client) and a Telnet server destination port.

Parameter	Setting
Default Action (on Advanced screen)	Discard
Action (Filter action)	Pass
Protocol	TCP
TCP Flags	All
Src. Address Type	Host
Src. Address	Host 1's IP address
Src. Port	All
Src Port Value	1023
Src. Port Operator	>
Dest. Address Type	Host
Dest. Address	Host 2's IP address
Dest. Port	Telnet
Dest. Port Operator	==

Note RIP updates are also filtered out by these filters, so dynamic routing (using RIP) cannot function. This can be overcome by defining additional filters to allow RIP updates to pass. RIP uses UDP (port 520) for both source and destination. Alternatively, a static route to LAN 2 can be established in Router 1 and a static route to LAN 1 can be established in Router 2.

Internet access filters

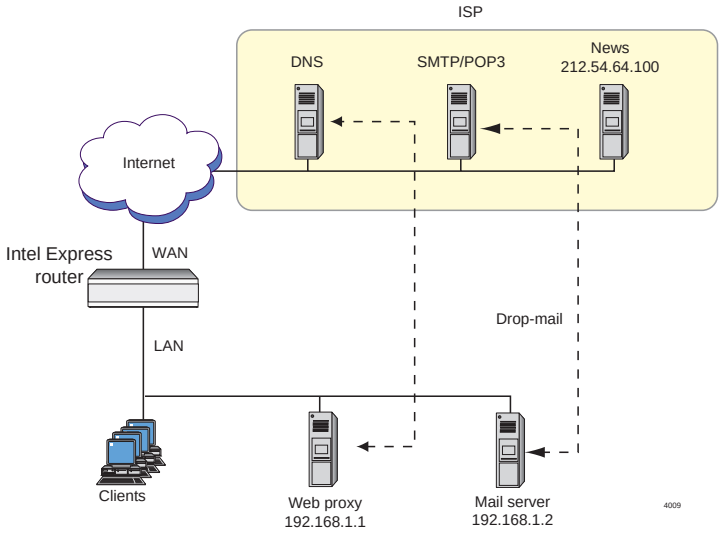
A brief description of the filters required to allow Internet access from devices on your LAN is given in "IP filters required for basic WWW access and services", p. 142.

Stateful Filter Examples

Protecting Your Private Network From the Internet With a Single LAN Port

Filtering requirements

This scenario uses stateful pass filters to create a firewall to protect your private network from the Internet while still giving users access to Internet services WWW (HTTP), FTP, e-mail (SNMP and POP3) and News (NNTP). The private network contains a Web proxy server and a mail server.



The mail server in this example is configured to use drop-mail for a domain.

Static route setup

Define a default static route on your connection to the Internet. The default static route setting has a network address of 0.0.0.0 and a subnet mask of 0.0.0.0. See “Static routes”, p. 200 for details.

Filters required

This example sets the firewall on the connection to the Internet on the WAN interface. Filters are not required on the LAN connection, so you can disable filtering on the LAN port.

Receive Filters on Connection to the Internet

Set the Default Action for traffic not filtered to Discard. This prevents any access from the Internet to your private network.

Transmit Filters on the Connection to the Internet

Configure these transmit filters on the connection to the Internet.

Filter and Function	Parameter	Setting
Discard all traffic not allowed to pass by specific filters.	Default Action	Discard
1 Allows DNS requests and replies from the Web proxy on the LAN.	Action	Stateful pass
	Protocol	UDP
	Src. Address Type	Host
	Src. Address	192.168.1.1
	Src. Port	All
	Dest. Address Type	All
	Dest. Port	DNS
	Dest.Port Value	53
	Dest. Port Operator	==
2 Allows DNS requests and replies from the Mail server on the LAN.	Action	Stateful Pass
	Protocol	UDP
	Src. Address Type	Host
	Src. Address	192.168.1.2
	Src. Port	All
	Dest. Address Type	All
	Dest. Port	DNS
	Dest. Port Value	53
	Dest. Port Operator	==
3 Allows ICMP messages between the Web server on the LAN and the Internet. This filter is optional - see note1)	Action	Stateful Pass
	Protocol	ICMP
	Src. Address Type	Host
	Src. Address	192.168.1.1
	Dest. Address Type	All

Filter and Function	Parameter	Setting
4 Allows ICMP messages between the Mail server on the LAN and the Internet. This filter is optional - see note1	Action	Stateful pass
	Protocol	ICMP
	Src. Address Type	Host
	Src. Address	192.168.1.2
	Dest. Address Type	All
5 Allows HTTP requests and replies from the Web proxy on the LAN.	Action	Stateful pass
	Protocol	TCP
	Src. Address Type	Host
	Src. Address	192.168.1.1
	Src. Port	All
	Dest. Address Type	All
	Dest. Port	HTTP
	Dest. Port Value	80
	Dest. Port Operator	==
6 Allows FTP requests and replies from the Web proxy on the LAN.	Action	Stateful pass
	Protocol	TCP
	Src. Address Type	Host
	Src. Address	192.168.1.1
	Src. Port	All
	Dest. Address Type	All
	Dest. Port	FTP control
	Dest. Port Value	21
	Dest. Port Operator	==
7 Allows News from the LAN to a specific News server on the Internet.	Action	Stateful pass
	Protocol	TCP
	Src. Address Type	All
	Src. Port	All
	Dest. Address Type	Host
	Dest. Address	212.54.64.100
	Dest. Port	NNTP
	Dest. Port Value	119
	Dest. Port Operator	==

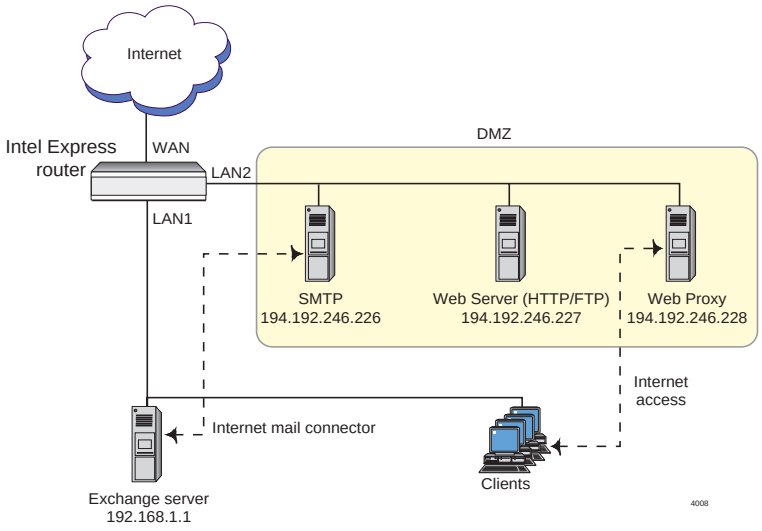
Filter and Function	Parameter	Setting
8 Allows SMTP requests and replies from the LAN to the Internet.	Action	Stateful pass
	Protocol	TCP
	Src. Address Type	Host
	Src. Address	192.168.1.2
	Src. Port	All
	Dest. Address Type	All
	Dest. Port	SMTP
	Dest. Port Value	25
	Dest. Port Operator	==
9 Allows POP3 requests and replies from the Web server on the LAN.	Action	Stateful pass
	Protocol	TCP
	Src. Address Type	Host
	Src. Address	192.168.1.2
	Src. Port	All
	Dest. Address Type	Host
	Dest. Port	POP3
	Dest. Port Value	110
	Dest. Port Operator	==

Note 1 This filter is optional. ICMP is used for IP status and control messages, such as with *ping*, which may useful in troubleshooting.

Setting Up a DMZ Firewall Using Two LAN Ports

Filtering requirements

This scenario illustrates the use of two LAN ports to set up firewall protection using stateful pass filters to protect your private network from the Internet. The private network is set up on the LAN1 port. A DMZ is set up on LAN2 that gives access to services required from the private network and the Internet. You configure IP filters to direct all traffic from LAN1 destined for the Internet through the services on LAN2. Any traffic from the Internet is filtered out or directed to services on LAN2.



Static route setup

Define a default static route on your connection to the Internet. The default static route setting has a network address of 0.0.0.0 and a subnet mask of 0.0.0.0. See “Static routes”, p. 200 for details.

Filters required

This example sets the firewall filtering on the connection to the Internet on WAN interface and the LAN1 connection. Filtering on the LAN2 connection is disabled.

Receive Filters on LAN1

These filters control the traffic from the LAN1 to the LAN2 services.

Filter and Function	Parameter	Setting
Discard all traffic not allowed to pass by specific filters	Default Action	Discard
1 Allows outgoing mail (SMTP) to the SMTP server on the DMZ. The filter is set to allow traffic from only the Exchange server.	Action	Stateful pass
	Protocol	TCP
	Src. Address Type	Host
	Src. Port	All
	Src. Address	192.168.1.1
	Dest. Address Type	Host
	Dest. Address	194.192.246.226
	Dest. Port	SMTP
	Dest. Port Value	25
	Dest. Port Operator	==
2 Allows HTTP traffic from all clients on LAN1 to the Web proxy on LAN2.	Action	Stateful Pass
	Protocol	TCP
	Src. Address Type	All
	Src. Port	All
	Dest. Address Type	Host
	Dest. Address	194.192.246.228
	Dest. Port	Other
	Dest. Port Value	8080 (see note 2)
	Dest. Port Operator	==
3 Allows ICMP messages from the Exchange server on the LAN1 to the SMTP server on the DMZ.	Action	Stateful Pass
	Protocol	ICMP
	Src. Address Type	Host
	Src. Address	192.168.1.1
	Dest. Address Type	Host
	Dest. Address	194.192.246.226

Note 2 It is common for Web proxies to use port 8080. However some servers, for example Microsoft Proxy§ Server, use port 80.

Transmit Filters on LAN1 Connection

These filters prevent unwanted traffic to the private network while allowing mail services through to the private network.

Filter and Function	Parameter	Setting
Discard all traffic not allowed to pass by specific filters.	Default Action	Discard
1 Allows incoming mail (SMTP) from the SMTP server on DMZ. The filter is set to allow traffic to the Exchange server on LAN1 only.	Action	Stateful pass
	Protocol	TCP
	Src. Address Type	Host
	Src. Address	194.192.246.226
	Src. Port	All
	Dest. Address Type	Host
	Dest. Address	192.168,1,1
	Dest. Port	SMTP
	Dest. Port Value	25
	Dest. Port Operator	==

Receive Filters on the Connection to the Internet

Configure these receive filters on the connection to the Internet. These filters direct traffic to the services on LAN2 (DMZ).

Filter and Function	Parameter	Setting
Discard all traffic not allowed to pass by specific filters	Default Action	Discard
1 Allows incoming mail (SMTP) from the Internet to the SMTP server on the DMZ.	Action	Stateful pass
	Protocol	TCP
	Src. Address Type	All
	Src. Port	All
	Dest. Address Type	Host
	Dest. Address	194.192.246.226
	Dest. Port	SMTP
	Dest. Port Value	25
	Dest. Port Operator	==

Filter and Function	Parameter	Setting
2 Allows incoming WWW (HTTP) from the Internet to the Web server on the DMZ.	Action	Stateful pass
	Protocol	TCP
	Src. Address Type	All
	Src. Port	All
	Dest. Address Type	Host
	Dest. Address	194.192.246.227
	Dest. Port	HTTP
	Dest. Port Value	80
	Dest. Port Operator	==
3 Allows incoming FTP access from the Internet to the Web server on the DMZ.	Action	Stateful pass
	Protocol	TCP
	Src. Address Type	All
	Src. Port	All
	Dest. Address Type	Host
	Dest. Address	194.192.246.227
	Dest. Port	FTP control
	Dest. Port Value	21
	Dest. Port Operator	==

Transmit Filters on the Connection to the Internet

Configure these transmit filters on the connection to the Internet.

Filter and Function	Parameter	Setting
Discard all traffic not allowed to pass by specific filters	Default Action	Discard
1 Allows outgoing mail from the SMTP server on the DMZ to any SMTP server on the Internet.	Action	Stateful pass
	Protocol	TCP
	Src. Address Type	Host
	Src. Port	All
	Src. Address	194.192.246.226
	Dest. Address Type	All
	Dest. Port	SMTP
	Dest. Port Value	25
	Dest. Port Operator	==

Filter and Function	Parameter	Setting
2 Allows outgoing WWW (HTTP) from the Web proxy on the DMZ to any HTTP server on the Internet.	Action	Stateful pass
	Protocol	TCP
	Src. Address Type	Host
	Src. Address	194.192.246.228
	Src. Port	All
	Dest. Address Type	All
	Dest. Port	HTTP
	Dest. Port Value	80
	Dest. Port Operator	==
3 Allows outgoing FTP access from the Web proxy on the DMZ to any FTP server on the Internet.	Action	Stateful pass
	Protocol	TCP
	Src. Address Type	Host
	Src. Address	194.192.246.228
	Src. Port	All
	Dest. Address Type	All
	Dest. Port	FTP control
	Dest. Port Value	21
	Dest. Port Operator	==
4 Allows DNS requests from the servers on the DMZ to any DNS server on the Internet.	Action	Stateful pass
	Protocol	UDP
	Src. Address Type	All
	Src. Port	All
	Dest. Address Type	All
	Dest. Port	DNS
	Dest. Port Value	53
	Dest. Port Operator	==
5 Allows secure HTTP (HTTPS) from the Web proxy on the DMZ to any HTTP server on the Internet.	Action	Stateful pass
	Protocol	TCP
	Src. Address Type	Host
	Src. Address	194.192.246.228
	Src. Port	All
	Dest. Address Type	All
	Dest. Port	Other
	Dest. Port Value	443
	Dest. Port Operator	==

Network Address Translation (NAT)

Network Address Translation (NAT)

Network Address Translations can be used when connecting networks that are using private IP network addresses to the Internet, which requires public addresses. NAT can also be used to connect networks which are using the same network address.

Public IP addresses used on the Internet must be unique and are usually assigned by Internet Service Providers (ISPs). Private IP addresses used within a LAN can be unassigned, but must never be allowed on the public Internet. NAT allows you to translate between these two address types, even when the networks are of a different size or only a single public IP address is supplied by your ISP.

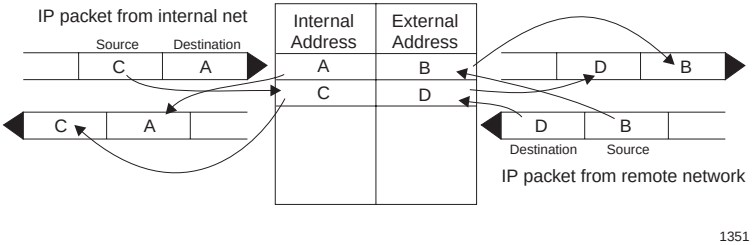
NAT table

NAT uses a Network Address Translation table which contains internal and corresponding external IP addresses. Each entry in the table can be either a network address, a subnet address or a single IP address.

For packets from the router, addresses matching entries in the internal list with the defined internal port are translated to the associated external addresses and port. For packets from the remote router, addresses matching entries in the external list with the defined external port are translated to the associated internal addresses and port.

Internal and external addresses

When an IP packet is translated by NAT, both the source and destination IP addresses and ports can be translated by different entries in the table, as shown in the following diagram:



For packets from the internal network, address A for either the source or destination IP address is translated to address B, and address C is translated to address D.

For packets from the external network, address B for either the source or destination address is translated to address A, and IP address D is translated to address C.

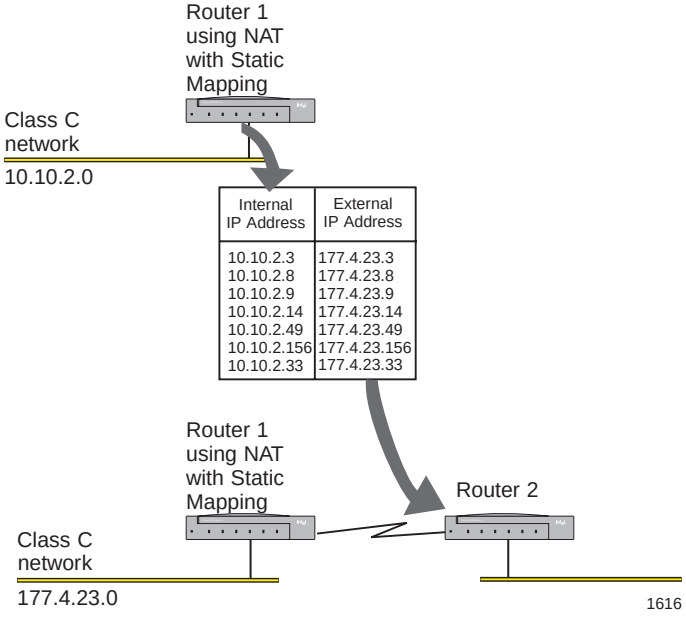
Mapping methods

NAT can use one of the following mapping methods:

Static Mapping

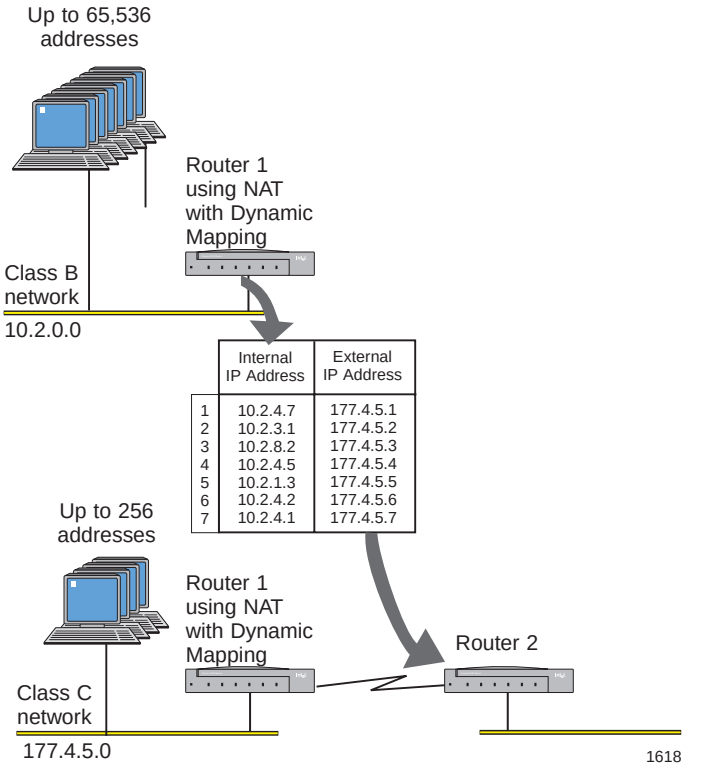
Static Mapping can be used to translate an internal network to an equal sized external network (for example a class C network to a class C network). Static Mapping, can also be used to translate individual internal IP addresses to external IP addresses.

When using Static Mapping, addresses are simply converted by translating the network part of the IP address between the internal and external address. The host part of the address remains the same. For example, an internal class C network address 10.10.2.8 (where 10.10.2 is the network part of the address) could be translated to the external class C network address 177.4.23.8 (where 177.4.23. is the network part of the address).



Dynamic Mapping

Dynamic Mapping can be used to translate between IP networks of different sizes, that is, a large internal network can be translated to smaller external network or vice versa. For example, a class B internal network could be translated to class C external network addresses. In this case, the entire internal address (network and host part) must be translated to an assigned external address. External addresses are therefore assigned sequentially as they are required.

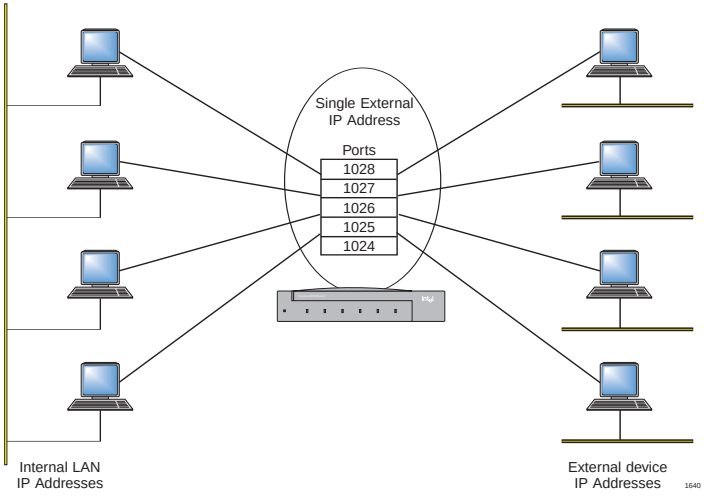


The diagram gives an example using Dynamic Mapping between an internal class B network (address 10.2.0.0) and an external class C network address (address 177.4.5.0).

Single IP Address Mapping

Single IP address translation is available to allow a single IP address to be used by a full IP network. This is typically used when connecting to the Internet where only a single unique IP address is obtained from the Internet Service Provider (ISP).

Single IP address translation uses port mapping to assign the available port numbers of a single IP address to different IP addresses. This allows multiple simultaneous TCP/IP sessions via the single address.



If access to devices for specific internal services are required from external sources, a static translation must be set up to allow access to the TCP port on the internal network device. A typical example of this is an e-mail server on the internal network which receives mail from an external server. A static NAT table entry must be defined to allow access to the SMTP port (port 25) on the internal e-mail server. Otherwise, the external e-mail server will not be able to send mail to the internal server.

Internally initiated communications only

Note When using dynamic mapping and single IP addressing NAT, only internal networks can initiate communications with external devices. An external device does not know the address of the internal device until it has been informed of it by a packet from the device. For this reason, static links must be established to internal network devices and ports that you wish to make accessible to the external network.

Using an internal proxy with NAT

If NAT is used together with an internal proxy for Internet access, single network IP address mapping should be used to map the proxy host to the IP address supplied by the Internet Service Provider (ISP). In this case, the proxy will take care of address-port mapping between the internal IP addresses and the ports of the external IP address.

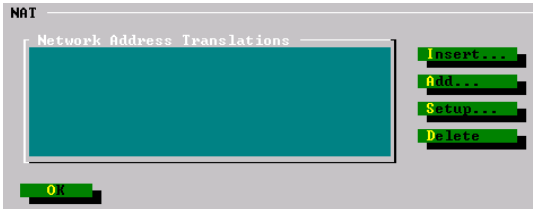
Setting Up Network Address Translations on the LAN and WAN Links

To configure IP Network Address Translation (NAT) on a link

Follow this procedure to configure IP NAT on a LAN or WAN link of the router.

1 Enter the `Advanced` screen for the IP link and select `NAT`.

From the Advanced Setup main display, select `Protocols` > `IP` > select the `link` > `Setup` > `Advanced` >`NAT`.

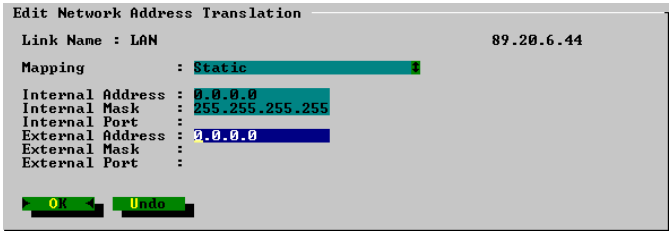


2 Add or edit an exiting entry according to the following:

- Use `Add` to add a new NAT entry after the selected entry.
- Use `Insert` to add a new NAT entry before the selected entry.
- Use `Setup` to edit a selected entry.

Note The order that NAT entries are defined may be relevant. The address of IP packets will be translated using the first entry in the list which matches an address (source or destination) of the packet.

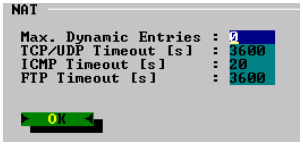
3 Configure the NAT entry as required by your installation.



- For static mapping, the External subnet mask is taken from the `Internal Mask` as the network sizes must be the same.
- To translate your network IP address to a single external IP address, set `Mapping` to `Network to Single IP`. If the external IP address is dynamically assigned by your Internet Service Provider (ISP), set the `External Address` to `0.0.0.0` with the `External Mask` of `255.255.255.255`. Otherwise set the External Address and Mask to the static external IP address or address range.
- To give access to internal network devices (for example e-mail servers) when using a single external IP address, set Mapping to `Static Port (Single IP)` and specify the `Internal Address` and the `Internal and the External Port` required for the service. For example, set the `Internal Address` to the address of your e-mail server and the `Internal` and `External Port` to 25 to allow communications between an internal and external access e-mail servers using SMTP (which uses port 25).

4 Repeat these steps to configure Network Address Translations on the other LAN and WAN links as required.

5 Select NAT on the `IP` > `Advanced` screen and set the advanced NAT parameters for the router if required.



These parameters are only relevant for single IP address NAT and can be used to limit the number of dynamic port reassignments and for timing out dynamic assignments.

Examples of Use

Simple address translation

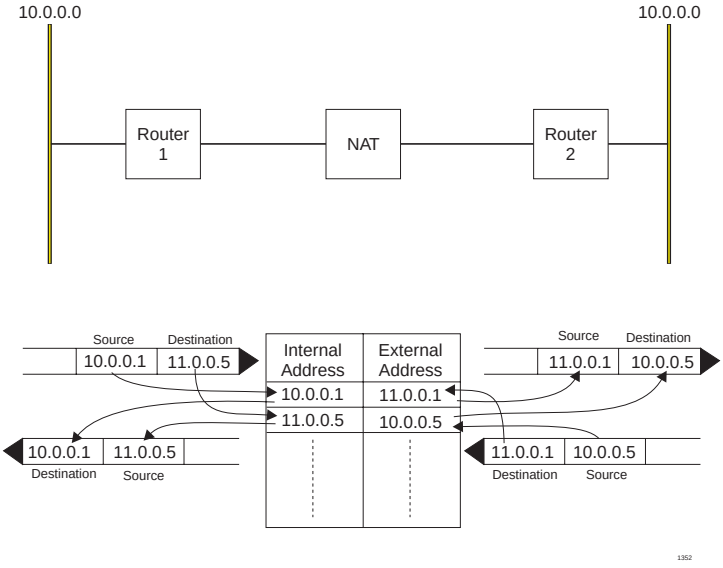
A common application of NAT is simple address translation between private internal network addresses and public external network addresses. This can be done to connect your network using private IP addresses (which are not allowed on the Internet) to the public Internet, which requires the use of officially assigned IP addresses, to avoid renumbering an entire network which uses unreserved IP addresses.

NAT is often used where only a single IP address is supplied by your Internet Service Provider (ISP) for use by a number of devices on your LAN. By using single IP address NAT, internal IP addresses are mapped to different port numbers of the external IP address, allowing many devices to use the single IP address simultaneously.

NAT also offers some simple security by not displaying your internal LAN IP addresses to external networks.

NAT between networks with the same network number

When using NAT, it is possible to have a number of networks which use the same network number. In this case, an artificial network number is created to which packets are addressed. Two NAT entries are made to convert the source and destination IP addresses of packets transmitted between the two networks (see the following example).



Each network will use a non-existent IP network address (11.0.0.0) to communicate with the remote network. The NAT table will translate addresses in packets transferred between the networks to the actual network addresses 10.0.0.0. in the above example.

Translation table entries

For the above example, the entries required in the NAT table are:

- Entry 1
  - Mapping: Static
  - Internal Address: 10.0.0.0
  - Internal Mask: 255.0.0.0
  - External Address: 11.0.0.0

- Entry 2
  - Mapping: Static
  - Internal Address: 11.0.0.0
  - Internal Mask: 255.0.0.0
  - External Address: 10.0.0.0

Configuring IP Static Routes

Static routes

You should establish static routes if you want to route data to a few destinations without using the Routing Information Protocol (RIP). RIP updates, which are transmitted between routing devices, can take valuable link bandwidth particularly over slow WAN links. By disabling RIP and establishing static routes to the required destinations, RIP updates are eliminated from the link, thereby reserving all the available bandwidth for data communications. RIP can be a particular problem over on-demand links, such as X.25 SVCs, where RIP updates can prevent the link from being timecut.

Static routes are only practical for small networks. For larger networks, RIP must be used to keep track of network topology changes. In this case, consider using triggered RIP instead. Triggered RIP alleviates the problems over on demand links, where RIP updates prevent the link from being timecut.

Static routes must also be established if the router cannot dynamically build a route to the destination.

Static routes are announced to other routing devices using RIP. If other routes with lower metrics to the destination network are available, the route with the lowest metrics is used.

To configure IP static routes for the router

Follow this procedure to configure IP static routes for the router.

1 Select `Static Routes` on the `IP` screen.

From the Advanced Setup main display, select `Protocols`> `IP`.

2 Add and configure the static routes required for you installation.

Use `Add` to add new static routes or `Setup` to edit existing static routes.

- The `Network Address`, `Network Mask` and the router `Link` on which the network can be reached must be defined. For static routes via the LAN link, the `Forward Address` of the next router to the destination network must also be defined.
- For host routes, used to connect directly to a single host over a link, the IP address of the host is entered for the `Network Address` and the `Network Mask` is set to `255.255.255.255` to specify a single IP address.

Note When using IP RIP routing over an Internet Tunnel a static host route to the IP address of the remote router must be established on the link in the router to the ISP. The tunnel will not be stable otherwise.

Domain Name System (DNS)

Domain Name System server

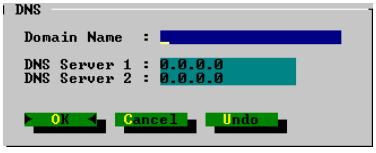
If a Domain Name System (DNS) server is available on your network, you can configure the DNS into the Express Router.

A DNS server allows the router to use domain names, for example www.intel com, instead of IP addresses to identify devices. The router Log System can use this feature when sending messages to a Syslog server. See “Configuring the Log System”, p. 253.

To configure the Express Router for DNS

Follow this procedure to configure the router for a Domain Name Server (DNS).

1 From the advanced Setup main display, select `Protocols>IP>DNS`.



2 Configure the DNS parameters.

Parameter	Description
`Domain Name`	Enter the domain name, for example, abc.xyz.com.
`DNS Server 1`	IP address of the primary DNS server.
`DNS Server 2`	IP address of the secondary DNS server.

8 Configuring Novell IPX Routing

Introduction to Novell IPX Routing in the Express Router

IPX Routing

IPX routing in the Express Router is used to forward IPX traffic addressed to devices on the networks accessible to the router through LAN and WAN links.

Dynamic Routing using RIP and SAP

Routing Information Protocols (RIP) and Service Access Protocol (SAP) are used to transmit network topology information and service access information between routing devices. This enables routers to automatically determine which networks and services are accessible and the best routes between them.

Routing using RIP and SAP is known as dynamic routing. The network will automatically establish itself and dynamically adapts itself to changes.

Static routing

Static routes are routes to remote networks which must be manually configured in the router. That is, the route is defined and is not discovered dynamically by the router using the Routing Information

Protocol. By disabling RIP and establishing static routes to the remote networks over the WAN links, routing traffic can be eliminated from the WAN links.

This is useful for slow WAN links in order to maximize the available bandwidth for data traffic. Routing using static routes is only really practical for small internetworks. For larger internetworks, the router needs to dynamically keep track of network topology changes, and the use of dynamic routing (RIP and SAP) is recommended.

IPX WAN Protocol

Select the IPX WAN Protocol if it is supported by the router over the WAN link.

The IPX WAN Protocol ensures consistency for operation with the router over the WAN link if the router over the link uses the IPX WAN Protocol. The IPX WAN Protocol must be either enabled or disabled in both the routers over the WAN link.

IPX Watchdog Packets over X.25 SVCs

Use of IPX Watchdog spoofing

The use of IPX watchdog spoofing is highly recommended over on-demand (switched) X.25 SVCs, otherwise the operating costs could become excessive.

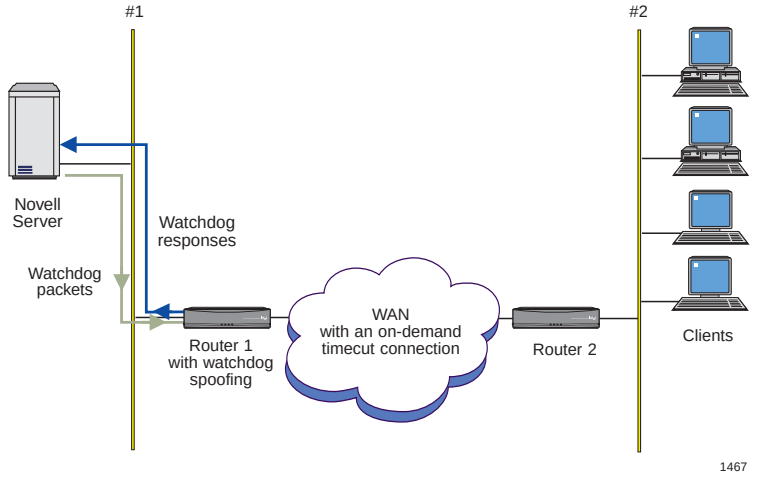
Watchdog packets

When a NetWare§ client has not communicated with a server within a predefined time interval, the server sends out a watchdog packet to the client to ask if it is still connected. If a client fails to respond to a predefined number of watchdog packets, the session is terminated at the server.

Problems with IPX watchdog packets occur when communication between NetWare clients and a server is over on-demand (switched) X.25 SVCs. If a number of clients are operating over the link, the link may never get the chance to become inactive so the operating costs can be high. In addition, if the link is brought down for some reason, the client sessions may be terminated prematurely. This problem also occurs with IPX/SPX keep-alive packets See “SPX Keep-alive Packets over X.25 SVCs”, p. 205.

IPX watchdog spoofing

To counteract the problem of sending watchdog packets over on-demand links, IPX watchdog spoofing can be set up in the router before the link (on the server's side). When IPX watchdog spoofing is enabled, the router answers IPX watchdog packets on behalf of clients. The link is therefore not activated to send IPX watchdog packets to clients.



SPX Keep-alive Packets over X.25 SVCs

Use of SPX spoofing

The use of SPX spoofing is highly recommended over on-demand (switched) X.25 SVCs. Otherwise, the operating cost of these type links could be excessive.

SPX Keep-alive packets

When using the IPX/SPX protocol, the keep-alive function is taken care of by the SPX transport protocol, rather than by IPX watchdog packets. As with IPX, SPX uses keep-alive packets to keep sessions alive—when an established session has not communicated within a predefined time interval, SPX keep-alive packets are used to determine if the session is still established. If an established session fails to respond to a predefined number of SPX keep-alive packets, the session is terminated.

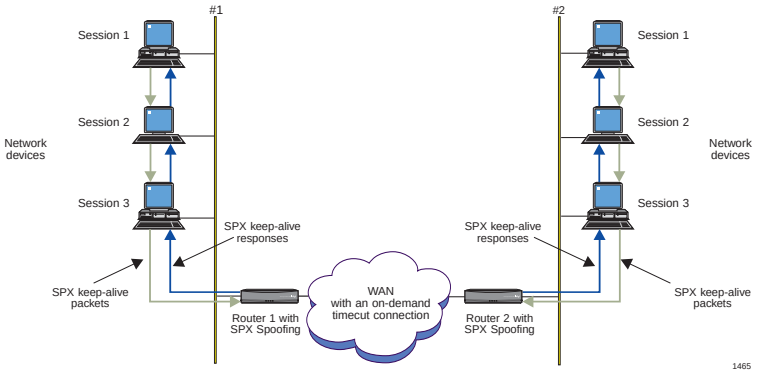
As with IPX watchdog packets, SPX keep-alive packets cause problems when operating over on-demand link. See “IPX Watchdog Packets over X.25 SVCs”, p. 204. Unlike IPX watchdog packets, SPX keep-alive packets can be sent by all the NetWare devices in the session.

SPX spoofing

To counteract the problem of sending SPX keep-alive packets over X.25 SVCs, SPX spoofing can be set up in the routers over the link.

Note SPX spoofing must be enabled in both routers over the link for it to be effective.

When the X.25 SVC is timecut and SPX spoofing is enabled, the router answers SPX keep-alive packets on behalf of devices over the link. The link is not activated just to send SPX keep-alive packets.



Configuring IPX Routing on the LAN and WAN Links

To configure IPX routing on the LAN and WAN links

Follow this procedure to configure IPX routing:

Note All the configuration parameters in `Advanced Setup` are described in on-line help. To access help for a parameter, click on the parameter and press the `F1 Help` key.

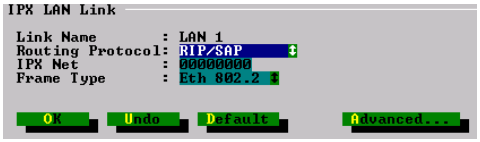
1 Enter the `Protocols` option of Advanced Setup.

2 To enable IPX routing services, click on the `IPX Routing` check box on the `Protocols` screen. IPX routing is enabled if the check box is marked with an asterisk [*] and disabled if the check box is empty [ ].

3 Select `IPX` on the `Protocols` screen.

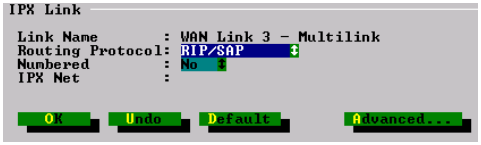
4 Use `Add` to add IPX routing to a LAN or WAN link or `Setup` to edit the IPX routing configuration for an existing link.

- The IPX setup screen for the LAN link:



The `IPX Net` number and `Frame Type` in use on your LAN must be defined for the LAN link.

- The IPX setup screen for WAN links:

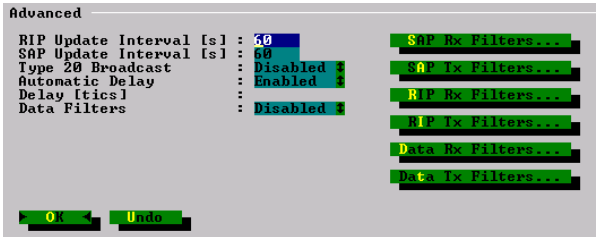


If dynamic routing is to be used over the link, the `Routing Protocol` must be set to `RIP/SAP`. Set the `Routing Protocol` to `None/Static` to disable dynamic routing and establish static routes and services via the link. See “Configuring IPX Static Routes and Services”, p. 220.

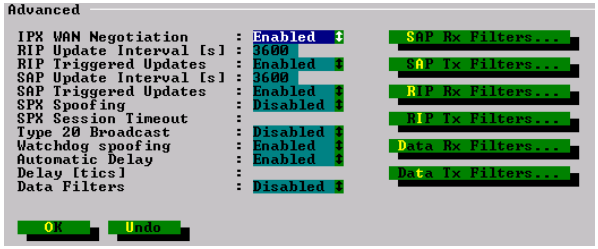
A numbered link (where an IPX network number is assigned to the WAN link) is normally only used when required by the remote router over the link.

5 Select `Advanced` on the link screen and set up any advanced link parameters and features required.

The `Advanced` screen for the LAN link:



The Advanced screen for WAN links:



- If NetBIOS requires forwarding by the router, enable `Type 20 Broadcasts` on the link.
- For on-demand X.25 SVCs links enable SPX Spoofing and IPX Watchdog Spoofing if required. See “IPX Watchdog Packets over X.25 SVCs”, p. 204 and “SPX Keep-alive Packets over X.25 SVCs”, p. 205.

  An SPX spoofing session timeout interval can also be defined when SPX spoofing will be disabled allowing SPX clients to answer their SPX keep-alive packets as usual. IPX Watchdog spoofing is not normally required on permanent WAN links such as PPP leased lines, Frame Relay links, and X.25 Permanent Virtual Circuits (PVCs).
- Enable Filtering if IPX filtering is required on the link. Setting up IPX data filters (accessed by selecting `Data Rx Filters` and `Data Tx Filters`) is described in “Configuring IPX Data Filtering on the LAN and WAN Links”, p. 216.

  Setting up IPX RIP and SAP filters is described in “RIP and SAP Filters”, p. 210.

RIP and SAP Filters

RIP and SAP filtering

Routing and service access information entering and leaving the Express Router can be filtered to remove unwanted routing and service access information. For example, this may be done to:

- restrict access to networks and services
- reduce the amount of routing and service information traffic

Implementation

RIP and SAP filters are implemented for both WAN and LAN links, and are implemented for both received (Rx) and transmitted (Tx) routing information.

RIP Rx filters

Use RIP Rx filters to remove selected incoming routing information before it is entered into the routing table for the router. Routing destinations removed in this way are not accessible via the router, and the routing information is not passed on to other routers.

RIP Tx filters

Use RIP Tx filters to remove selected routing information before it is passed on to other routers. Routing destinations removed in this way are accessible via the router but the routing information is not passed on to other routers.

SAP Rx Filters

Use SAP Rx Filters to remove selected incoming service access information before it is entered into the service information table for the router. Services removed in this way are not accessible via the router, and the service information is not passed on to other routers.

SAP Tx Filters

Use SAP Tx Filters can be used to remove selected service access information before it is passed on to other routers. Services removed in this way are accessible via the router but the service information is not passed on to other routers.

Configuring RIP and SAP Filtering on the LAN and WAN Links

To configure RIP and SAP filtering on the LAN and WAN links

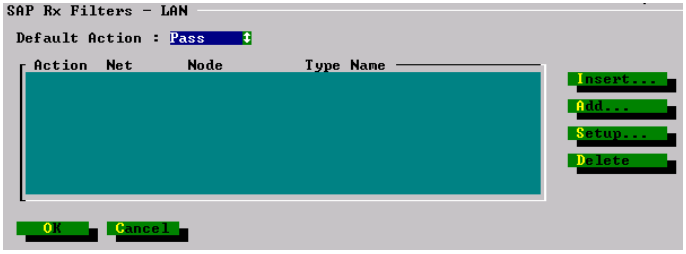
Follow this procedure to configure IPX filtering on the LAN and WAN links for the router (from the `Advanced` screen for the link).

1 Enter the `Advanced` screen for the IPX link.

From the Advanced Setup main display, select `Protocols` > `IPX` > select the link > `Setup` > `Advanced`.

2 Select `SAP Rx Filters` on the Advanced screen for the IPX link to define SAP receive filters.

SAP receive filters pass or discard service access information before it enters the services table for the router.

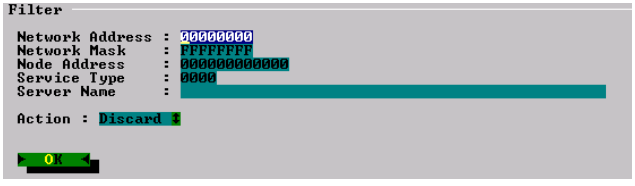


Set the `Default Action` according to the following:

- Set to `Discard` to discard all service access information coming from the link which is not allowed to pass by specific filters.
- Set to `Pass` to pass all service information unless discarded by specific filters.

3 Add and configure the SAP Rx filters as required for your installation.

Use `Add` to add a new filter after the selected filter, `Insert` to add a new filter before the selected filter, or `Setup` to edit the selected filter.



Define the filter criteria as required, see “SAP Rx and Tx filter criteria”, p. 213.

4 Select `SAP Tx Filters` from the `Advanced` screen for the IPX link to define SAP transmit filters.

SAP transmit filters pass or discard outgoing service access information on the link.

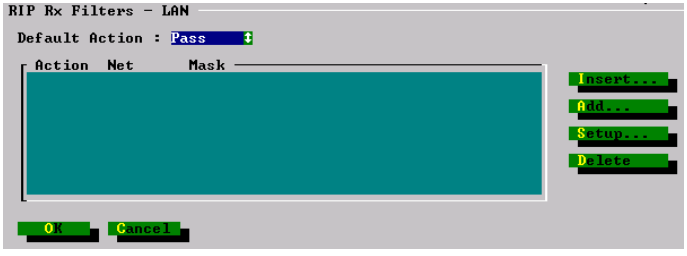
Set the `Default Action` according to the following:

- Set to `Discard` to discard all service access information for transmission on the link which is not allowed to pass by specific filters
- Set to `Pass` to pass all service access information unless discarded by specific filters.

The procedure for setting up receive (Rx) and transmit (Tx) SAP filters is the same, see step 3.

5 Select `RIP Rx Filters` on the `Advanced` screen for the IPX link to define RIP receive filters.

RIP receive filters pass or discard network access information before it enters the services table for the router.



Set the `Default Action` according to the following:

- Set to `Discard` to discard all network access information from the link which is not allowed to pass by specific filters.
- Set to `Pass` to pass all network access information unless discarded by specific filters.

6 Add and configure the RIP Rx filters required for your installation.

Use `Add` to add a new filter after the selected filter, `Insert` to add a new filter before the selected filter, or `Setup` to edit the selected filter.

Define the filter criteria as required, see “RIP Rx and Tx filter criteria”, p. 214.

7 Select `RIP Tx Filters` from the `Advanced` screen for the IPX link to define RIP transmit filters.

RIP transmit filters pass or discard outgoing network access information on the link.

Set the `Default Action` according to the following:

- Set to `Discard` to discard all network access information for transmission on the link which is not allowed to pass by specific filters.
- Set to `Pass` to pass all network access information unless discarded by specific filters.

The procedure for setting up receive (Rx) and transmit (Tx) RIP filters is the same. See step 5.

SAP Rx and Tx filter criteria

Each SAP filter in the Express Router can be set up to pass or discard service information which is received (Rx filters) or transmitted (Tx filters) using the Service Access Protocol (SAP), based on the following criteria:

Network Addresses

Service access information can filter a single network address, or range of network addresses specified by the Network Address and Network Mask parameters.

When the Network Mask parameter is set to FFFFFFFF, service access will be filtered to a single Network Address. For other values of the Network Mask, a range of network addresses will be filtered. For

example, with a Network Address of ABC00000 and a Network Mask: FFF00000, service information will be filtered from/to all servers on the networks beginning with ABC.

Node Address

Service access information can be filtered from/to a single device (Node) address instead of network addresses.

Service type

To filter specific service types from any network or Node Addresses specified. The Reference Manual on the Intel Device View CD-ROM lists the Novell service type codes. To access the Reference Manual from Intel Device View, select Reference Manual from the Help menu.

Server Name

Service access information can be filtered from/to a single device identified by its unique server name.

RIP Rx and Tx filter criteria

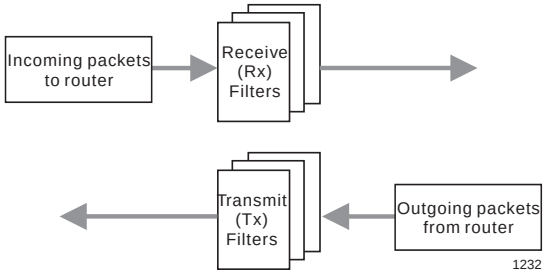
Each RIP filter in the Express Router can be set up to pass or discard network access information which is received (Rx filters) or transmitted (Tx filters) using the Routing Information Protocol (IPX RIP), based on a single network address, or range of network addresses specified by the `Network Address` and `Network Mask` parameters.

When the `Network Mask` parameter is set to FFFFFFFF, service access will be filtered from/to a single `Network Address`. For other values of the `Network Mask`, a range of network addresses will be filtered. For example, with a `Network Address` of 00000000 and a `Network Mask` of FFFFFF00, routing information will be filtered from/to all network numbers below 00000100 (between 00000001 and 000000FF).

IPX Data Filters

IPX data filters

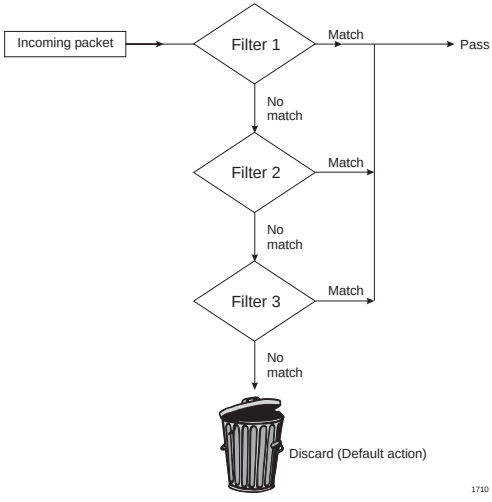
IPX data filters are defined on a link basis in the Express Router, and separate filters are implemented for transmit (for restricting IPX packets leaving the router on a link), and receive (for restricting IPX packets entering the router from a link).



Note A good understanding of IPX is required before effective filtering can be set up on the router. Filters must be defined as strictly as possible to eliminate unauthorized access to services, hosts and networks.

Packet processing by filters

If the default filter action for a link is set to discard, all incoming (for Rx filters) or outgoing (for Tx filters) IPX data packets on the link will be discarded unless otherwise allowed to pass by a filter. The following shows how data packets are processed by the IPX filters.



Packets are compared with filters in the order they are defined in the list. If a packet matches more than one filter, it will be processed by the first matching filter only.

If the default filter action for a link is pass, all incoming (for Rx filters) or outgoing (for Tx filters) IPX data packets on the link will be allowed to pass unless otherwise discarded by a filter.

Configuring IPX Data Filtering on the LAN and WAN Links

To configure IPX filtering on the LAN and WAN links

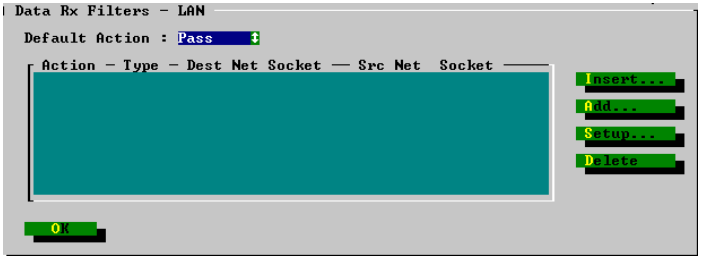
Follow this procedure to configure IPX filtering on the LAN and WAN links for the router to filter packets as they are received from the link or before they are transmitted on the link.

1. Enter the `Advanced` screen for the IPX link.

   From the Advanced Setup main display, select Protocols > IPX > select link > `Setup` > `Advanced`.

2. Set the `Data Filters` parameter to `Enabled` on the `Advanced` screen for the IPX link.

3. Select `Data Rx Filters` on the `Advanced` screen to define receive filters. Receive filters pass or discard incoming traffic from the link.



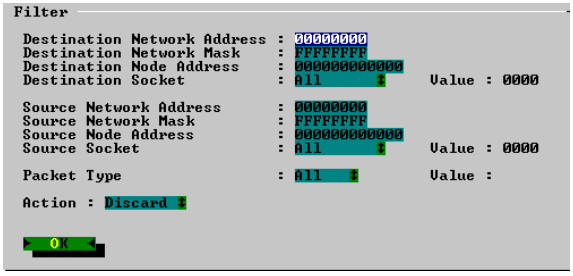
   Set the `Default Action` according to the following:

   - Set to `Discard` to discard all data from the link which is not allowed to pass by specific filters.
   - Set to `Pass` to pass all packets except packets discarded by specific filters.

4 Add and configure the IPX data filters required for your installation.

Use `Add` to add a new filter after the selected filter, `Insert` to add a new filter before the selected filter, or `Setup` to edit the selected filter.

Note Packets will be filtered using the first filter in the list which matches the packet, therefore the order can be relevant.



Define the filter criteria as required, see “IPX data filter criteria” following.

5 Select `Data Tx Filters` from the `Advanced` screen for the IPX link, to define transmit filters. Transmit filters pass or discard outgoing traffic on the link.

The procedure for setting up receive (Rx) and transmit (Tx) filters is the same. See step 3.

IPX data filter criteria

Each filter in the Express Router can be set up to pass or discard IPX packets based on the following criteria:

Note All the filter criteria defined are used.

Destination Network Addresses

IPX data traffic addressed to a single destination network address, or range of network addresses specified by the Destination Network Address and Destination Network Mask parameters can be filtered.

When the Destination Network Mask parameter is set to FFFFFFFF, packets addressed to the single Destination
Network Address specified will be filtered. For other values of the Destination Network Mask, data packets addressed to a range of network addresses will be filtered. For example, with a Network Address

of ABC00000 and a Network Mask: FFF00000, service information will be filtered from/to all servers on the networks beginning with ABC.

Destination Node Address

IPX packets addressed to a single device (node) can be filtered. A Destination Node Address of 000000000000 disables filtering on the destination node address.

Destination Socket

IPX packets addressed to specific sockets can be discarded. The most common IPX sockets (`NCP`, `NetBIOS`, `NLSP` and `IPX Ping`) can be selected from a list. Other sockets can be filtered by selecting `Other` for the `Destination Socket` and then entering the socket number `Value`.

Source Network Addresses

IPX data traffic from a single source network address, or range of network addresses specified by the `Source Network Address` and `Source Network Mask` parameters can be filtered.

When the `Source Network Mask` parameter is set to FFFFFFFF, packets from the single `Source Network Address` specified will be filtered. For other values of the `Source Network Mask`, data packets from a range of network addresses will be filtered. For example, with a `Network Address` of 00000000 and a `Network Mask` of FFFFFF00, routing information will be filtered from/to all network numbers below 00000100 (between 00000001 and 000000FF).

Source Node Address

IPX packets from a single device (node) can be filtered. A `Source Node Address` of 000000000000 disables filtering on the source node address.

Source Socket

IPX packets from a specific source socket can be discarded. The most common IPX sockets (`NCP`, `NetBIOS`, `NLSP` and `IPX Ping`) can be selected from a list. Other sockets can be filtered by selecting `Other` for the `Source Socket` and then entering the socket number `Value`.

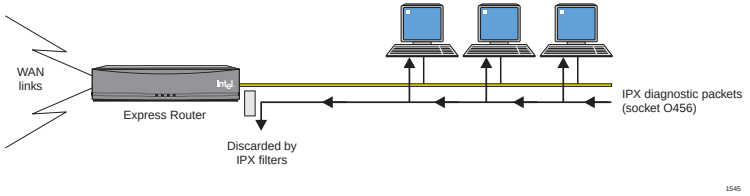
Packet Type

Specific IPX packet types can be filtered. NCP and SPX packets can be selected from a list. Other packet types can be filtered by selecting `Other` for the `Packet Type` and then entering the socket number `Value`.

IPX Filters Example

Filter requirement

NetWare devices use Diagnostic Request Packets to get information about other reachable devices. These packets can be used for testing if a device is reachable and gathering configuration information about devices. Diagnostic Request Packets can be broadcast to all devices and require each device to respond and can cause WAN links to become saturated. It is therefore sometimes desirable to eliminate these diagnostics from WAN links. This is done using the IPX data filters implemented in the Express Router.



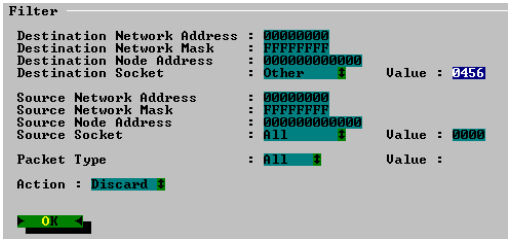
Note IPX ping may be affected by these filters, depending on whether the implementation of ping in the device which is testing for connectivity uses the diagnostics responder.

Filter Required

To discard diagnostic packets from the LAN so that they are not transmitted on WAN links, set up a filter on the LAN link:

- Set the default `Action` for the IPX Rx (receive) LAN filters to `Pass` to allow all data traffic to enter the router unless discarded by a filter.
- Set up an IPX Rx Filter for the IPX LAN link with the following criteria:
  - Set the filter `Action` to `Discard`

- Set the `Destination Socket` to `Other` and the `Destination Socket Value` to `0456` (the NetWare socket number for diagnostic packets)



Configuring IPX Static Routes and Services

IPX Static routes

You should establish static routes and services if you want to route data to a few destinations without using the Routing Information Protocol (RIP) and Service Access Protocol (SAP). RIP and SAP updates which are transmitted between IPX devices can take valuable link bandwidth, particularly over slow WAN link. By disabling RIP and SAP and establishing static routes to the required networks and services, RIP and SAP updates are eliminated from the link, thereby reserving all the available bandwidth for data communications. RIP and SAP can be a particular problem over on-demand (switched) X.25 SVCs links, where RIP and SAP updates can prevent the link from being timecut.

Static routes are only practical for small networks, for larger networks, RIP and SAP must be used to keep track of network topology changes and the availability of services. In this case, consider increasing the RIP and SAP update interval over X.25 SVC links instead.

Static services must also be established if the router cannot dynamically build a route to the destination.

Static routes and services are announced to other routing devices using RIP and SAP. Static routes can be prioritized to always use the static route or to use the best route (static backup route).

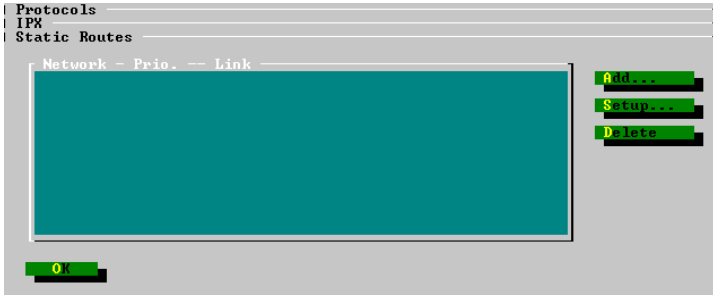
To configure Static Routes and Services

To configure IPX static routes and services for the router

Follow this procedure to configure IPX static routes and services for the router.

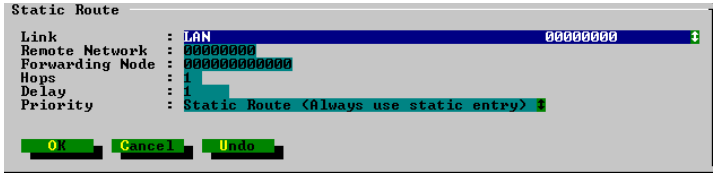
1 Select `Static Routes` on the `IPX` screen.

From the Advanced Setup main display, select `Protocols` > `IPX` > `Static Routes`.



2 Add and configure static routes as required by your installation.

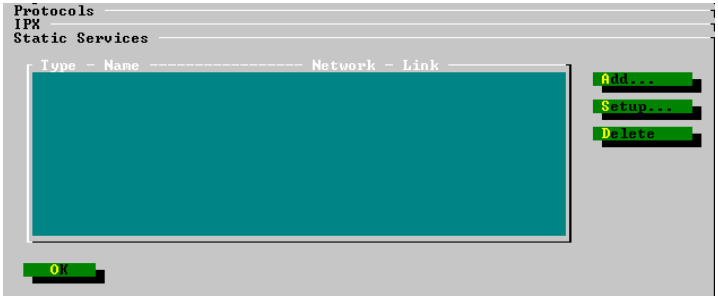
Use `Add` to add new static routes or `Setup` to edit an existing selected static routes.



- The `Remote Network` and the router `Link` on which the network can be reached must be defined.
- For primary static routes, which should always be used by the router, the `Priority` should be set to `Static Route (Always use static entry)`. For backup static routes, which should only be used if a better route is not available, set the `Priority` to `Static Backup Route (Use best route)`.

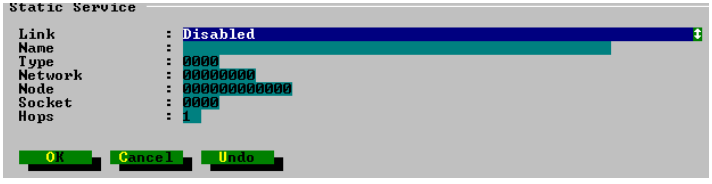
- For static routes via the LAN link, the `Forward Node` (address) of the next hop router to the destination network must also be defined.

3 Return to the `IPX` and select `Static Services`.



4 Add and configure static services as required by your installation.

Use `Add` to add new static services or `Setup` to edit selected existing static services.

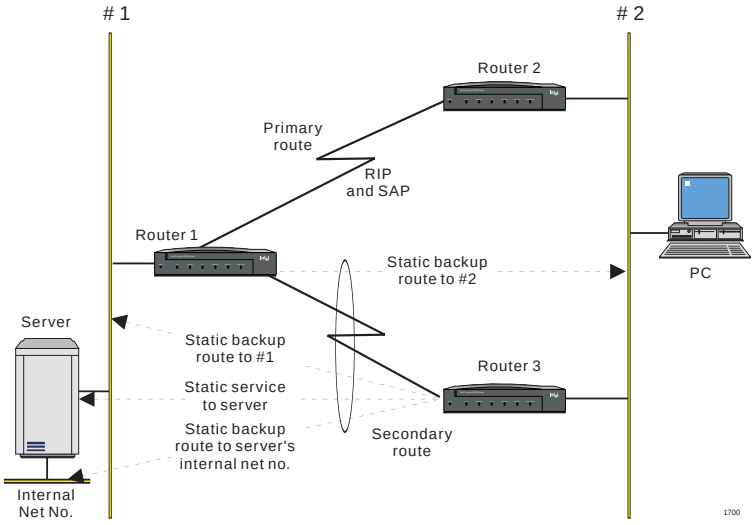


The `Network`, `Node`, `Socket` and the router `Link` on which the service can be reached must be defined.

Static Routes and Services Example

Example use of a Static Backup Route

A typical example of the use of static backup routes is shown in the following diagram of access and general backup access between network 1 and 2. In addition, the PC on network 2 requires access and backup access to the server on network 1:



Example description

The example is configured as follows:

- The primary link from network 1 to network 2 is the main route between network 1 and 2. This link uses dynamic routing (RIP and SAP).
- The secondary link between router 1 and router 3 is used as a static backup route between network 1 and 2, which is only used if the primary route fails. To allow general access between networks 1 and 2 in case the primary link should fail:
  - a static backup route to network 1 is configured in router 3
  - a static backup route to network 2 is configured in router 1

- To allow the PC to access the server on network 1, an additional static backup route to the internal network number of the server and a static service to the server must be established in router 3.

  Novell IPX servers use an internal network number which must be used when routing information to the server.

- For correct operation, the metrics for the backup routes must be higher than those for the primary route. To establish the static backup routes (in routers 1 and 3), dynamic routing over the backup link must be disabled and the static backup routes should be configured to `Use best route`. These routes are then only used if the primary route fails.

9 Configuring Bridging Services

Introduction to Bridging in the Express Router

WAN Bridging

Bridging services are available in the Express Router for forwarding data which is not routed by the routing protocols. Data is not forwarded by the router if:

- the routing protocol is not supported (the router supports IP RIP and IPX RIP/SAP)
- the routing protocol is not enabled in the router
- the routing protocol is not set up for use on the appropriate LAN and WAN links in the router.

Spanning Tree Algorithm

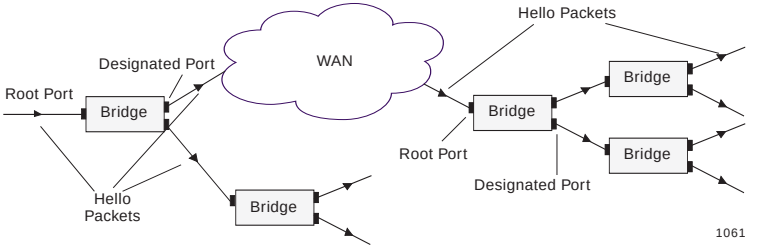
The Spanning Tree Algorithm is implemented for bridging in the router. The Spanning Tree Algorithm gives the possibility of having redundant paths within a bridged environment; this is not allowed in a non-spanning tree environment as data could be forwarded between networks segments via multiple paths without any coordination.

The Spanning Tree Algorithm allows stand-by bridges to be implemented which are ready to start forwarding packets if another bridge is removed from the network (powered off or fails during operation).

Bridge Spoofing

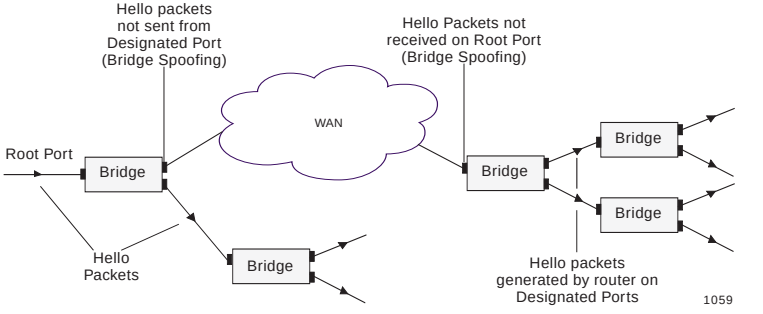
Hello packets over WAN links

Hello packets (Configuration BPDU packets) are used by the Spanning Tree Algorithm to track changes in the bridged network topology. These packets take up valuable bandwidth on WAN links, and are a particular problem when communicating over on-demand links, such as X.25 SVCs. Configuration BPDU packets are sent from Designated Ports to Root Ports at intervals defined by the Hello Time in the Root Bridge (2 seconds as the default). These configuration BPDU packets can prevent on-demand from becoming timecut—the operating costs are then excessive.



Bridge Spoofing

To counteract the problem of Configuration BPDU packets taking up excessive WAN link bandwidth, the Express Router implements Bridge Spoofing. When Bridge Spoofing is set up in the bridges on either side of a WAN link, the WAN link is not used to send configuration BPDU packets unless a network topology change is detected.



Configuring Bridging Services on the LAN and WAN Links

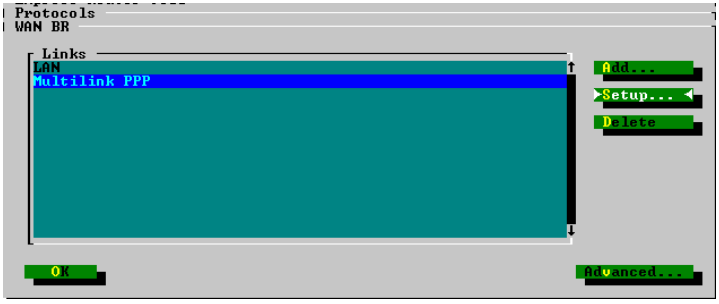
To configure bridging on the LAN and WAN links

Follow this procedure to configure bridging services:

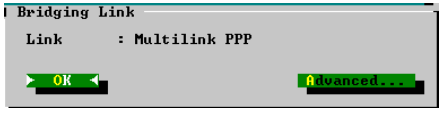
1 Enter the `Protocols` option of Advanced Setup.

2 Enable WAN Bridging services by clicking on the `WAN Bridging` check box on the `Protocols` screen. Bridging services are enabled if the check box is marked with an asterisk `[*]` and disabled if the check box is empty `[ ]`.

3 Select `WAN BR` on the `Protocols` screen.

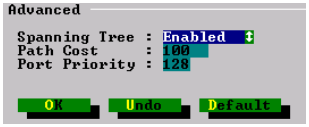


4 Use `Add` to add bridging to a LAN or WAN link or `Setup` to edit the bridging configuration for an existing link.



5 Select `Advanced` on the `Bridge Link` screen to change the Spanning Tree parameters for the link.

The Advanced screen for the LAN link is as follows:

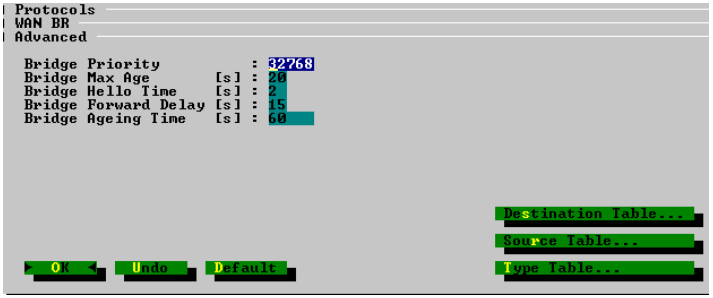


The Advanced screen for a WAN link is as follows:

- Set the `Spanning Tree` parameter to `Disable` if spanning tree is not required on the link.
- For WAN links, if the router over the WAN link is NOT an Intel router, set the `Spoofing` parameter to `Disabled`.
- The `Path Cost` and `Port Priority` parameters are used to set the priority for use of the link within the spanning tree and should generally be set to their default values.

6 Repeat steps 4 and 5 to configure bridging on any other LAN and WAN links.

7 Return to the WAN BR screen and select `Advanced` to set up the spanning tree parameters for the bridge if necessary.



These parameters are used by the Spanning Tree Algorithm when determining the priority for use of the Express Router

within the spanning tree and for becoming the root bridge of the spanning tree.

In most cases, the default values of these parameters should be used.

Configuring Static Destinations, Sources and Packet Types

Forwarding tables

Forwarding Tables are used when deciding where incoming packets should be bridged to. Forwarding tables can be permanently defined (static) or built by the router by learning the MAC addresses of devices on the LAN and WAN links. The following forwarding tables are implemented in the router:

Unicast Destination Forwarding Table—can contain both learned and static (user-defined) destinations for Unicast packets

This table contains Unicast destination MAC addresses on the associated LAN and WAN links which can be both learned by the router or defined during configuration of the router (static). Static Unicast destination entries can be defined to only allow packets on certain links or to discard packets to certain destinations.

The table can be set up to discard all packets to defined Unicast destinations unless allowed to pass by specific table entries. Bridge learning can be disabled so that only static (user-defined) Unicast destination MAC addresses will be forwarded.

Multicast Destination Forwarding Tables—static destinations for Multicast packets

This table can contain static Multicast destination MAC addresses and the incoming and outgoing links on which packets with the Multicast destination MAC addresses are permitted. The Multicast destination entries can also be set up to discard packets with certain Multicast destinations.

The table can be set up to discard all packets with Multicast destinations unless allowed to pass by specific table entries.

Source Forwarding Table—static destinations for source addresses

This table can contain static source MAC addresses and the incoming and outgoing links on which packets from the address are permitted. The static source MAC address entries can also be set up to discard packets from defined source MAC addresses.

The table can be set up to discard packets with Multicast destinations from all source addresses which are not allowed to pass by specific table entries.

Type Forwarding Table—static destinations for Ethernet packet types

This table contains static Ethernet packet types and the incoming and outgoing links on which the packet types are permitted. Static type entries can also be set up to discard defined packet types.

The table can be set up to discard all packet types unless allowed to pass by specific table entries.

The Reference Manual on the Intel Device View CD-ROM lists known Ethernet packet types. To access the Reference Manual from Intel Device View View, select `Reference Manual` from the Help menu.

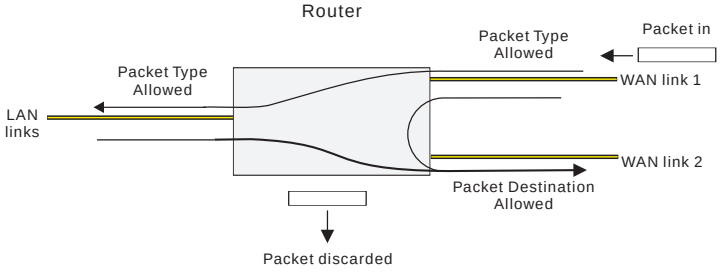
Packets are processed by all the forwarding tables in the router. A frame which is allowed to pass by one table may be discarded by another.

Static Forwarding Table Example

Forwarding example 1

An incoming packet is received by the router for bridging on WAN link 1. The packet has a destination MAC address of 000080000001, a source MAC address of 000080000002 and a packet type code of 1234. It is processed as follows:

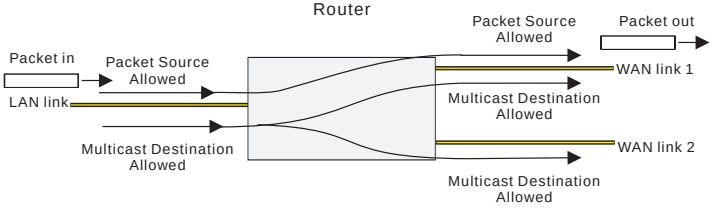
1. It is checked for loop-back. The packet has not been sent on the link on which it has just been received so it passes the loop-back test without being discarded.
2. The packet has a Unicast destination MAC address so it is checked against the entries in the Unicast Destination Forwarding Table. An entry is found in the table for a destination MAC address of 000080000001. All incoming links are always used by the Unicast Destination Table. The entry defines the outgoing link as WAN link 2.
3. The source MAC address of the packet is checked against the entries in the Source Forwarding Table and is not found.
4. The packet type code (1234) is checked against the entries in the Type Forwarding Table. An entry is found for packet type 1234 with an incoming link of WAN link 1. The entry defines the outgoing link as the LAN links.
5. The packet is discarded as the Unicast Destination Forwarding Table only allows the packet to be forwarded on link 2 and the Type Forwarding Table only allows the packet on the LAN link. The packet is therefore incompatible with both these conditions at the same time.



Forwarding example 2

An incoming packet is received by the router for bridging on the LAN link. The packet has a destination MAC address of 010080111111, a source MAC address of 000080222222 and a packet type code of 4321. It is processed as follows:

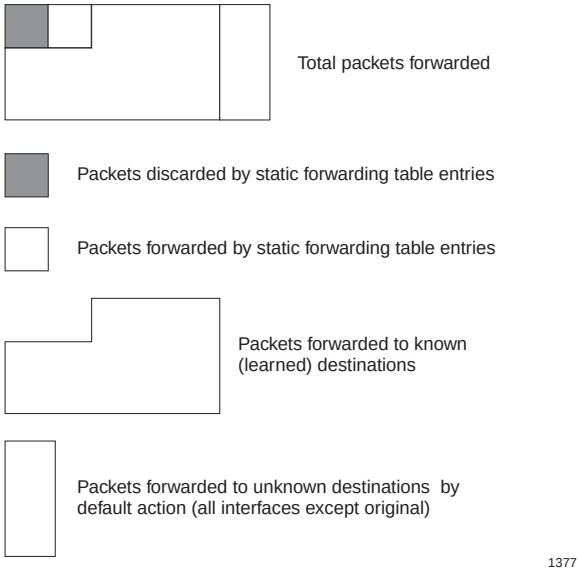
1. It is checked for loop-back. The packet has not been transmitted on the link on which it has just been received so it passes the loop-back test without being discarded.
2. The packet has a Multicast destination MAC address and so is checked against the entries in the Multicast Destination Forwarding Table. Two entries are found in the table for a destination MAC address of 010080111111 and the incoming link as the LAN link. One of the entries defines the outgoing link as WAN link 1, the other defines the outgoing link as WAN link 2. The packet is therefore labelled for forwarding on both the WAN links.
3. The source MAC address of the packet is checked against the entries in the Source Forwarding Table. An entry is found for a source MAC address of 000080222222 with the incoming link as the LAN link. The entry defines the outgoing link as WAN link 1.
4. The packet type code (4321) is checked against the entries in the Type Forwarding Table and is not found. The Type Forwarding Table default action is set to pass so the packet is not discarded.
5. The packet is forwarded on WAN link 1 because the source MAC address is not allowed to forward packets to WAN link 2 by an entry in the Source Forwarding Table.



Controlled Bridging

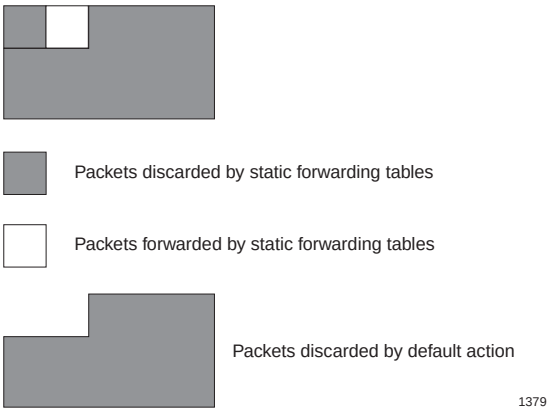
Controlled bridging

Conventional bridging forwards packets to destinations that the bridge learns about with a number of packets being forwarded and discarded by the static forwarding table.



The diagram shows how much data gets forwarded (unshaded area) out of the total number of packets received for bridging.

The Express Router can be configured to discard packets which are not allowed to pass by entries in the forwarding tables. In addition, the learning function can be disabled so that the bridge forwarding tables only contain the static (user-defined) entries. When set up in this way, the bridge only forwards packets addressed to defined destinations, from defined sources and with defined Ethernet packet types. That is, all packets are discarded unless they are allowed to pass by static forwarding table entries.



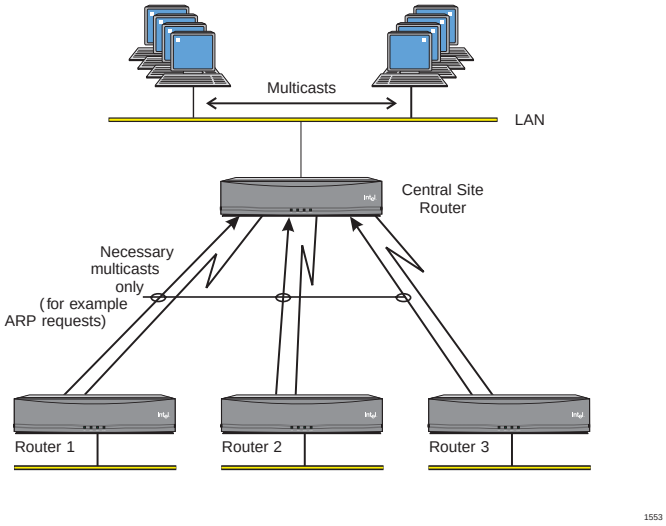
The above diagram shows how much data gets forwarded (unshaded area) out of the total number of packets received for bridging when using controlled bridging—bridge learning is disabled and the default action of the Destination, Source and Type Forwarding Tables is set to discard.

This way of controlling bridged data traffic can be used for security purposes and restrict the bridged data traffic over expensive WAN links.

Restricting Multicasts to Remote Networks

Discard Multicast packets from unknown sources

The Express Router has a feature which prevents Multicast packets from unknown source MAC addresses from being forwarded over WAN links. Use this feature when a central site router is communicating with a number of remote devices.



The Default Action in the central site router is set to `Discard Multicast`, and the MAC addresses of the remote routers are allowed to pass by filter entries. This allows necessary remote Multicast packets (which use the MAC address of the router) to be forwarded by the router while all local Multicasts are discarded without being transmitted on the WAN links.

Typically, the default action of the Destination Forwarding Table is set to Discard to prevent stations that the router does not know about from being Multicast to all destinations.

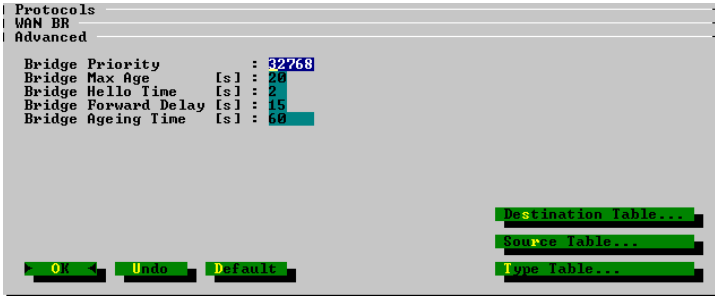
Configuring Static Tables and Controlled Bridging

To configure static tables and controlled bridging

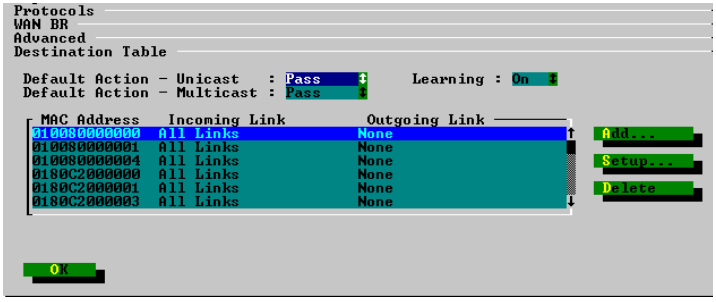
Follow this procedure to configure static forwarding tables (filters) for the bridging services in the router.

1 Enter `WAN BR` screen and select `Advanced`.

From the Advanced Setup main display, select `Protocols` > `WAN BR` > `Advanced`.



2 Select `Destination Tables` on the `Advanced` screen for bridging to define both Unicast and Multicast static destinations for the bridge.



Certain Multicast addresses are discarded by default. The Reference Manual on the Intel Device View CD-ROM explains this. To access the Reference Manual from Intel Device View View, select `Reference Manual` from the Help menu.

- Set the `Default Action Unicast` to `Discard` to discard all Unicast packets unless allowed to pass by entries in the table (static and learned destinations).

- Set the `Default Action Multicast` to `Discard` to discard all Multicast packets unless allowed to pass by entries in the table (static only).
- Set the `Learning` parameter to `Off` to disable bridge learning. If the `Default Action` parameters are set to `Discard`, data packets are then only forwarded to static (user-defined) destinations. This is known as controlled bridging.

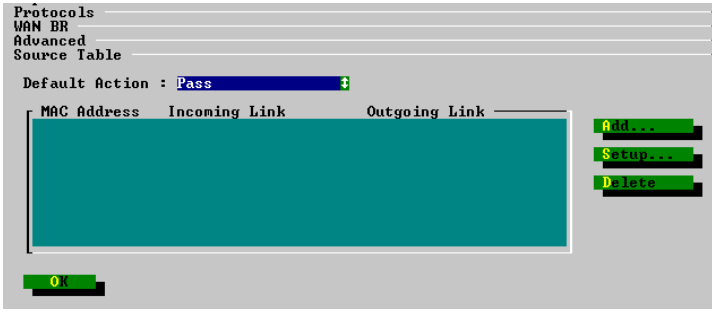
3 Add and configure the destination table entries (both Unicast and Multicast) required for your installation.

Use `Add` to add new entries or `Setup` to edit selected existing entries.

Configure the `Destination` parameters as required according to the following:

Parameter	Description
`MAC Address`	To specify the MAC address of the static destination. This address can be either a Unicast or Multicast MAC address.
`Incoming Link`	Frames having the defined destination MAC address arriving on the links defined here are authorized for forwarding to the defined Outgoing Link by the Destination Forwarding Table. If a Unicast MAC address is defined above, this parameter must be set to `All Links`.
`Outgoing Link`	Frames having the defined destination MAC address arriving on the defined Incoming Links are authorized for forwarding to the links defined here. For Multicast destinations, if this parameter is set to `None`, the `Incoming Link` must be set to `All Links`.

4 Return to the `Advanced` screen and select `Source Tables` for bridging to define both static sources for the bridge.

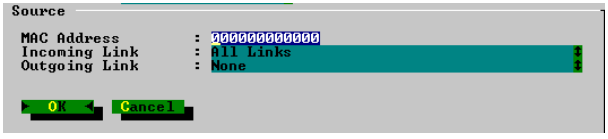


Set the `Default Action` according to the following:

- Set to `Discard Multicast` to discard Multicast packets from all source addresses unless allowed to pass by entries in the table. See “Restricting Multicasts to Remote Networks”, p. 235
- Set to `Pass` to pass packets from all source addresses unless discarded by specific filters.

5 Add and configure the Source Table entries required for your installation.

Use `Add` to add new entries or `Setup` to edit existing entries.

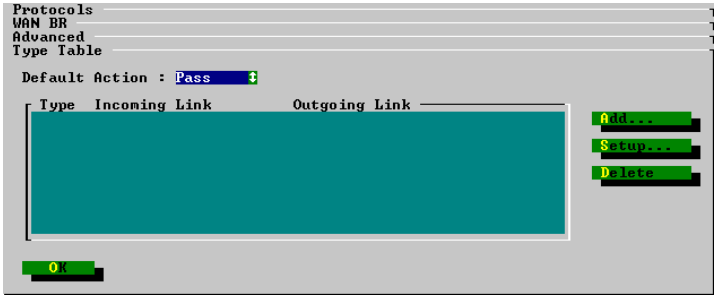


Configure the `Source` parameters as required according to the following:

Parameter	Description
`MAC Address`	Specifies the MAC address of the static source.

Parameter	Description
`Incoming Link`	Frames having the defined source MAC address arriving on the links defined here are authorized for forwarding to the defined `Outgoing Link` by the Source Forwarding Table.
`Outgoing Link`	Frames having the defined destination MAC address arriving on the defined `Incoming Links` are authorized for forwarding to the links defined here. If `None` is selected, the `Incoming Link` must be set to `All Links`.

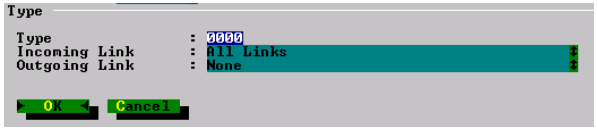
6 Return to the `Advanced` screen for bridging and select `Type Tables` to define both static sources for the bridge.



Set the `Default Action` to `Discard` to discard all Ethernet packet types unless allowed to pass by entries in the table.

7 Add and configure the Type Table entries required for your installation.

Use `Add` to add new entries or `Setup` to edit selected existing entries.



Configure the static frame type parameter as required.

Parameter	Description
`Type`	Specifies the Ethernet Type Code for the frames on the static path.
`Incoming Link`	Frames having the defined Ethernet frame type arriving on the links defined here are authorized for forwarding to the defined `Outgoing Link(s)` by the Type Forwarding Table.
`Outgoing Link`	Frames having the defined Ethernet frame type arriving on the defined `Incoming Links` are authorized for forwarding the links defined here. Set this to `None` to discard the defined frame type from the `Incoming Link`.

10 Configuring the DHCP Server

Overview

DHCP Server

The DHCP (Dynamic Host Configuration Protocol) Server automates the assignment of IP addresses and other network information to client devices connected to your network, such as PC workstations or servers.

The DHCP Server services both local and remote clients and can be configured to dynamically:

- assign an IP address including a subnet mask, and gateway address (IP address of this router).
- assign a defined DNS (Domain Name System) address.
- assign a defined WINS server (Windows Internet Name Service).

The DHCP server is configured with a range of IP addresses. During initial startup, and periodically thereafter, clients request and receive this information from the DHCP Server (see “DHCP Lease Time”, p. 242).

The DHCP provides an efficient way to assign and manage your IP Address allocation, eliminating the need to manually configure addresses for each device on your network.

DCHP IP Addresses

The DHCP Server can be configured with a range of IP addresses:

- Public addresses assigned by an Internet Service Provider for use on the public Internet.
- Private IP addresses for use within your network only.

DHCP Lease Time

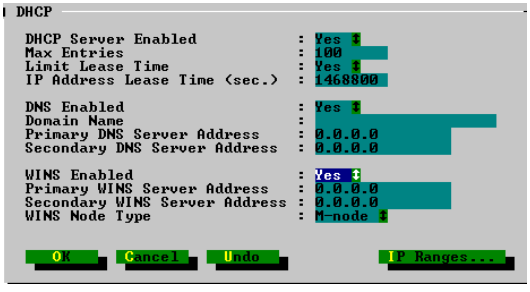
You can configure the DHCP server to assign IP addresses on a lease time basis. That is, the clients use an IP address for a defined period of time and then it must check in with the DHCP server. This gives the DHCP server the opportunity to update the client with any configuration changes. The DHCP server can then renew the client's address lease or assign a new IP address as required.

Configuring the DHCP Server

To configure the DHCP Server

Follow this procedure to configure the DHCP Server.

1 From the Advanced Setup main display, select `Protocols` > `IP` > `DHCP`.



2 Configure the DHCP server parameters.

- To enable the DHCP server, set the `DHCP Server Enabled` parameter to `Yes` and configure the following:

Parameter	Description
`Max. Entries`	Defines the maximum number of IP addresses that can be allowed in the DHCP IP address table.
`Limit Lease Time`	Enables or disables the IP address lease time function.
`IP Address Lease Time`	Defines the amount of time (in seconds) a client can use an assigned IP address before checking in with the DHCP server. Range: 60-31,622,400 (60 seconds to 366 days)

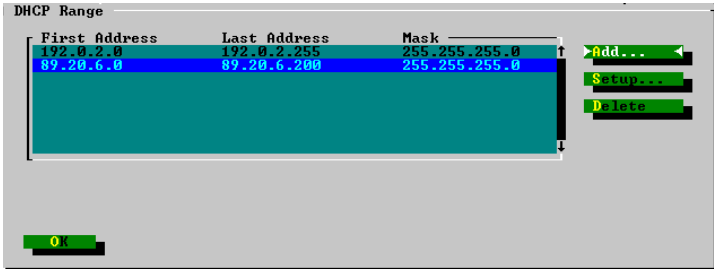
- To enable the DHCP server to assign a DNS address to clients, set `DNS Enabled` to `Yes` and configure the following:

Parameter	Description
`Primary DNS Server`	The IP address or your DNS server.
`Domain Name`	Your domain name, e.g., www.xyz.com (optional). Maximum 26 characters.
`Secondary DNS Server`	The IP address of your secondary DNS server, if in use.

- To enable the DHCP server to assign a WINS address client, set the `WINS Enabled` to `YES` and configure the following:

Parameter	Description
`Primary WINS Server Address`	The IP address or your WINS Server.
`Secondary WINS Server Address`	The IP address of your secondary WINS server, if in use.
`WINS Node Type`	WINS server node type (H, B, P, or M). The default is B, and is suitable for most installations.

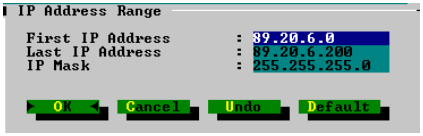
3 Select `IP Ranges` to configure the range of IP addresses available for assignment by the DHCP.



The screen lists the current IP ranges configured for the DHCP server.

- To add a new range, select `Add`.
- To edit an existing range, highlight the range and select `Setup`.

4 Configure the IP address range parameters.



The required parameters are:

Parameter	Description
`First IP Address`	The first IP address in the range that can be assigned by the DHCP server.
`Last IP Address`	The last IP address in the range that can be assigned by the DHCP server.
`IP Mask`	The subnet mask that is assigned to the client along with the IP address.

DHCP server considerations

These are some considerations and recommendations for configuring the DHCP server.

Reconfiguration

If you reconfigure the DHCP server, clients already assigned IP addresses are updated to the modification automatically, if the lease time option is enabled. The modification takes place when the clients lease on the IP address expires.

Disabling the DHCP server

If you disable the DHCP server, devices assigned IP addresses on a lease time basis may become inaccessible at the end of the lease period.

Remote Clients

In order to serve clients on remote LANs, you must define a range of IP addresses that matches the network address of the remote LAN. Ensure that DHCP server forwarding is enabled in the remote router.

Network Address Translation (NAT)

Disable NAT for links using the DHCP server.to avoid possible conflicts.

11 Management Access and Services

Management access and services

This chapter describes how to configure the following management access rights and services in the Express Router:

- SNMP/TFTP and Telnet access rights to the router
- Local Management passwords and access
- SNMP Trap destinations
- Management of the Log system messages
- Value added services - licensed software

Configuring Management Access Rights

Management access to the router

Monitoring and configuration of the router is normally done from Intel Device View. Intel Device View uses Simple Network Management Protocol (SNMP) to manage and monitor the router. The router can also be managed from other SNMP applications. To configure the router, upgrade the software and upload reports and logs from the router, Trivial File Transfer Protocol (TFTP) services are used.

By default, there is unlimited access to the router for SNMP and TFTP. Advanced Setup allows you to configure restrictions on SNMP and TFTP access including:

- assigning a TFTP password.
- defining the network addresses having SNMP/TFTP access.

Configuring SNMP/TFTP and Telnet Access Rights

Management protocol considerations

For any group of network addresses, you can configure access rights to the router for the following protocols:

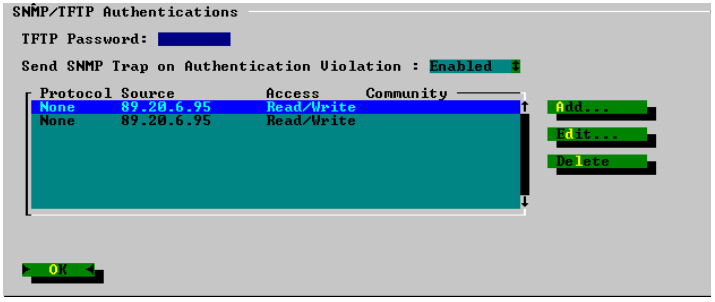
- SNMP - used for general monitoring of the router. SNMP is required to open a router from Intel Device View.
- TFTP - required to upload/download files to the router. TFTP is therefore required when configuring the router, for example, from Intel Device View using the Connection Setup.
- Telnet - required to access local management on the router via the LAN interface.

For full management and configuration capabilities, all three protocols must be configured.

To configure SNMP/TFTP access rights and passwords

To set up SNMP/TFTP management services and access rights in the router:

1 From the Advanced Setup main display, select `Management> Authentications`.



Note If there are no entries under the SNMP/TFTP Authentications, then no access restrictions exist. Once one or more entries are added, then only those entries apply. Separate entries must be made for each proto-

col (SNMP, TFTP, Telnet).

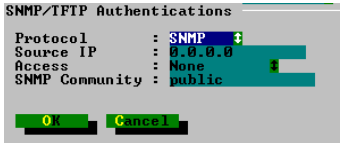
2 To assign a password for TFTP access to the router, enter the password in `TFTP Password` field.

This password will be requested before any configurations can be saved in the router, whether from Intel Device View or any other TFTP application.

3 To send an SNMP trap to the management station when an unsuccessful or illegal attempt to access the router occurs, set the `Send SNMP Trap on Authentication` parameter to `Enable`.

4 To define the network addresses authorized to access the router for management using SNMP, TFTP, or Telnet select:

- `Add` to add a new address(es).
- `Setup` to edit existing addresses.



Use the following table to configure the `SNMP/TFTP Authentication` parameters:

Parameter	Description
`Protocol`	Defines the protocol for which the entry has access rights. See “Management protocol considerations”, p. 248. For full management access to the router, both SNMP and TFTP are required. You must configure a separate entry for each.
`Source IP`	This is the IP address of the host from which SNMP, TFTP or Telnet requests are accepted. An IP address of 0.0.0.0 means all IP addresses are accepted.

Parameter	Description
`Access`	Defines the access rights for authentication entry. Selecting `None` blocks all access to management.
`SNMP Community`	The name of the SNMP community for the entry. This must be defined. If no name is entered then all community names are accepted.

Configuring Local Management Passwords and Access

Local Management passwords and Telnet access

You access Local Management by establishing a Telnet session to the router or via the console port of the router. You can configure these access restrictions:

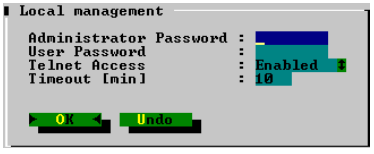
- Passwords having different restrictions for a normal user and administrator.
- Disable Telnet access from all devices on the network.

Note To deny Telnet access for specific devices or network addresses, see “Configuring SNMP/TFTP and Telnet Access Rights”, p. 248.

To assign Local Management passwords

To configure passwords for access to Local Management:

1 From the Advanced Setup main display, select `Management>Management`.



2 Enter the passwords for Local Management access as required. Passwords can be up to 8 characters.

- `Administrator Password` defines the password required to log in as an Administrator. An Administrator has access to monitoring and configuration.
- `User Password` defines the password required to log in as a User. A User has access to monitoring but not to configuration.

To configure Telnet access

To configure Telnet access to the router:

1 Select `Management` from the `Management` options screen.

2 To enable or disable Telnet access, set the `Telnet Access` parameter to the desired setting.

3 Enter the desired `Timeout` value (in minutes).

The `Timeout` parameter defines the length of time before a Telnet session is automatically closed due to lack of input from the user.

Note We recommend not to enter “0”. If set to “0”, the Telnet session will never timeout. This could present a problem if you lose the Telnet session. You will not be able to start a new session until the router is reset.

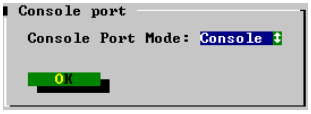
Setting the Console Port for Terminal Use - Console Mode

To set the console port for terminal use (Console mode)

To use the console port for Local Management access from a VT100-compatible terminal, the console port must be set to the console mode.

Note If the console port is currently configured for modem use, dial-up connections are disabled once you configure the console port to the console mode.

1 From the Advanced Setup main display, select `Management`> `Console port`.



2 Set Console Port Mode to Console Mode.

Configuring SNMP Traps

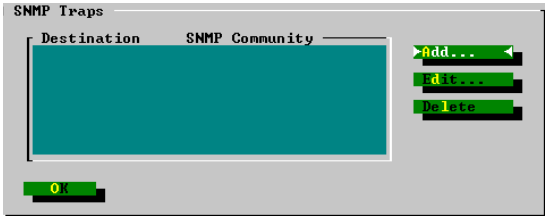
SNMP Traps

SNMP traps are generated by the router for normal router events, for example, links going up and down, and for operating problems. By default, Intel Device View will automatically set up the router to send SNMP traps to the PC on which it is running. You can configure additional destinations to send SNMP from Intel Device View or Advanced Setup.

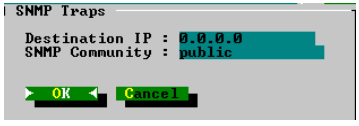
To define SNMP Trap Destinations

To define the destinations for SNMP traps generated by the router:

1 From the `Management` screen, select `Traps`.



2 Use `Add` to add a new trap destination and `Setup` to edit an existing destination.



Enter the `Destination IP address` and the `SNMP Community` string of the management station to receive the trap.

Configuring the Log System

Overview

Log System Configuration

The Log System of the router is a record of all system messages generated by the router. The Express Router offers these configuration features for managing the messages in Log System:

- Define messages to include in the log based on a defined criteria.
- Individually disable specific messages from appearing in the log (Discard Filter).
- Send log messages to a remote Syslog server.

Remote Storage to a Syslog

If a Windows or UNIX§ host on the network is running the Syslog daemon, you can configure the router to write the log messages to an ASCII file on that host.

Log System Messages

Log message fields

A log message consists of these fields:

Field	Description
Source	Protocol or feature affected by the error, such as PPP, Firewall.
Category	High-level classification of the message, such as security, accounting connectivity.
Level	Severity of the message.
ID	A number, which is used together with the source, that identifies a message (for example, PPP-3).
Date	Date and time of occurrence
Repeat Count	Number of occurrences for a particular message.
Description	An brief explanation of the event.

Log message levels

A log message can have these levels, listed in order of decreasing severity.

Level	Description
Fatal	Software or hardware failure; router is not operational.
Error	Operational error often caused by configuration mismatches or cabling. The router is operational but a specific function may not work correctly.
Note	A performance related problem. This indicates to the user that a function (local or remote) is not running optimally, for example.
Info	Informational type messages such as accounting, and links in time cut. No corrective action is required.
Debug	Very low-level message for debug purposes.

Configuring the Messages Included in the Log System

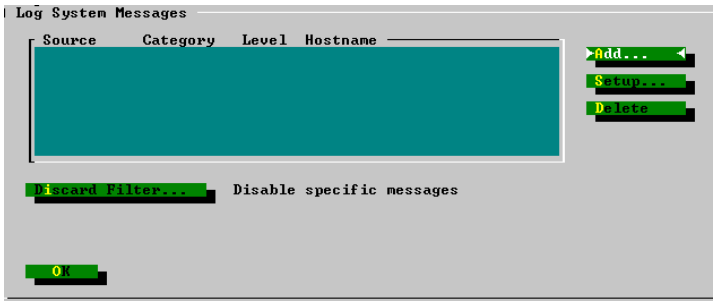
Log message inclusion criteria

By default all messages having a level of severity of `Note` and higher, regardless of Source or Category, are automatically stored in the Log. You can define which messages to include based on the following message fields: `Source`, `Category`, and `Level`.

To configure the messages included in the Log System and Syslog

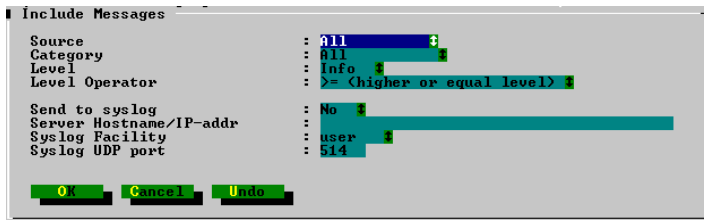
To configure the messages to include in the router Log System and send to a Syslog:

1 From the Advanced Setup main display, select `Management`> `Log System`.



The screen lists all the log inclusion entries currently configured.

2 Select `Add` to configure a new entry. To edit an existing entry, highlight the entry and select `Setup`.



3 To select the messages to include, define the criteria in the `Source`, `Category`, `Level`, and `Level Operator` fields.

4 To send the messages to a Syslog, set the `Send to Syslog` parameter to `Yes` and configure the following:

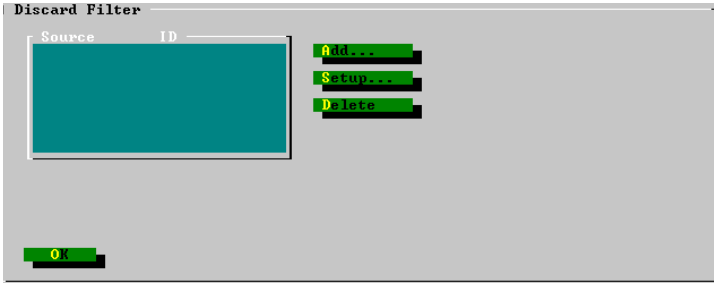
Parameter	Description
`Server Host name/ IP address`	The host name or IP address of the Syslog server to receive the messages. If you are using a host name, the router must be configured for DNS. See “Domain Name System (DNS)”, p. 202.
`Syslog Facility`	Defines the facility that is to receive the message on the Syslog server.
`Syslog UDP Port`	Defines the UDP (User Datagram Protocol) port to which to forward messages received by the Syslog.

To filter out individual messages from the Log System (Discard Filter)

You can filter specific messages from appearing in the Log System based on their Source and ID. This is called a Discard Filter. To define Discard Filters:

1 From the Advanced Setup main display, select `Management` > `Log System`.

2 Select `Log Filter`.



The screen displays all the current individual messages excluded from the log based on Source and ID.

3 Select `Add` to create a new exclusion entry. To edit an existing entry, highlight the entry and select `Setup`.

4 Select the `Source` from the drop-down list and enter the appropriate `ID` for the message.

Value-added Services

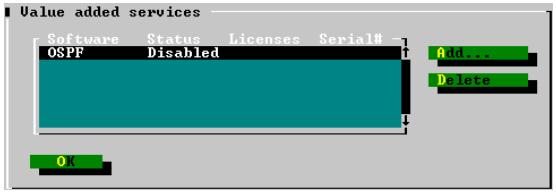
Value-added Services

There are a number of services and software features, such as OSPF, that you can purchase separately to enhance the functionality of the router. To activate these features, you must enter a license key which you receive upon purchase. In Advanced Setup, this is done using the Value-added Services option. You can also use this option to disable a license.

To activate a value-added service or licensed software

To activate a value-added service or licensed software, follow this procedure:

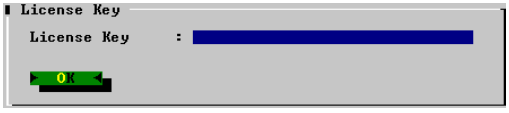
1 From the Advanced Setup main display, select `Management` > VAS.



The screen lists the features available for the router along with status information.

Field	Description
`Status`	The status of service. Enabled means the feature activated and disables means it is deactivated.
`Licenses`	This identifies the type of license that you have. 1 indicates a single device license. 10 indicates a ten device license. **Note:** The software cannot be activated on more devices than the number of licenses you have for the feature. See your software license agreement for details.
`Serial #`	The serial number assigned to the license by Intel.

2 Select the feature you want to activate, then select Add.



3 Type the license key and press Ok.

The license key can be found on your software license agreement. Type the license as it appears.

12 Gas Pump and Command Line Configuration

Introduction

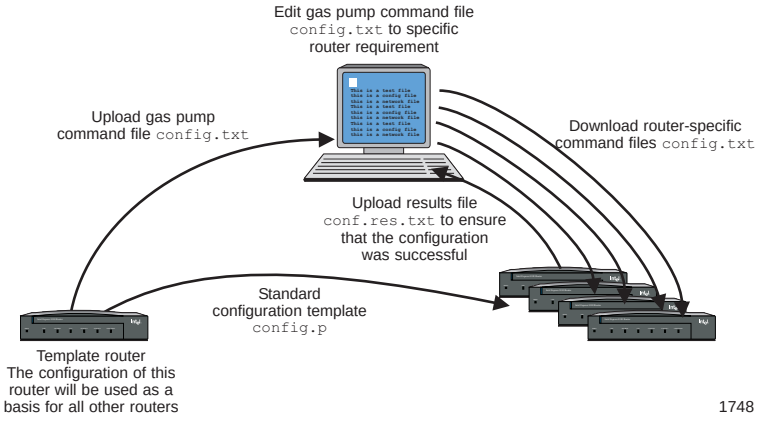
A command line interface is available from Local Management that provides limited configuration from a command prompt. The command line provides the ability to use TFTP to configure a number of routers based on the configuration of single template router (called Gas Pump configuration).

Gas pump and command line configuration of the router are intended for users that are experienced with the Express Router and those configuring a number Express Routers.

Gas Pump Configuration of the Router

Introduction to gas pump configuration of the router

Gas pump configuration is a type of batch configuration providing a quick way to setup a number of Intel Express Routers based on a pre-defined template configuration.



A router is first fully configured to the general requirements of the customer or remote user. The standard configuration is modified to installation-specific requirements using a file containing configuration commands (text file).

Note The commands that can be used in the configuration command file are limited to those required to set up an Internet link via a leased line or Frame Relay link.

The standard template configuration is first downloaded to the router being gas pump configured, followed by the configuration command file which modifies the standard configuration.

To access the router for gas pump configuration

Gas pump configuration of the router requires that you have TFTP (Trivial File Transport Protocol) access to the router to upload and download the gas pump configuration files. TFTP access to the router can be from any TFTP client.

Files used for gas pump configuration

The following files are used to gas pump configure a router:

Config.p

The config.p file is the configuration file of the router that will be used as the template configuration. When the template router has been configured, the Config.p file is obtained from it using TFTP. This file, containing the standard template configuration, is downloaded using TFTP to all routers being gas pump configured.

The Config.p file is a binary file and cannot be edited when it has been retrieved from the template router. The Config.p file must be transferred in binary mode.

Config.txt

This is a text file that contains configuration commands used to modify the standard configuration (config.p).

When the initial template router has been set up to work correctly, the Config.txt file is obtained from it using TFTP. Configuration parameters specific to each individual router are then changed in this file (using any standard text editor) before it is downloaded to the router being configured. Alternatively, it is possible to automatically generate the Config.txt configuration file (from a customer database for example) using scripts.

Note The Config.txt file must be downloaded to the router after the Config.p. The config.p does not take effect until the config.txt is downloaded.

Parameters typically configured for each router using the Config.txt file include:

- the external IP address of the router (as seen from the Internet)
- CHAP user ID and password
- the main (LAN) IP address of the router
- Frame Relay DLCIs.

Conf-res.txt

This is a text file that is retrieved from the router to report any errors that occurred during configuration of the router using the Config.txt file. This file should be retrieved from the first gas pump configured router to ensure that the gas pump configuration process is working correctly. Any errors reported in the Conf-res.txt file should be corrected and the process repeated until no errors are reported.

The file contains:

- the line number in the config.txt file of each command processed
- the result: `OK`, `INFO` or `ERROR`
- the command itself
- a summary of the results.

Viewing and editing the gas pump configuration text files

The files used for gas pump configuration of the router are viewed and edited using a standard text editor or using the Report Manager in Intel Device View.

To gas pump configure routers

This is the general procedure for gas pump configuring routers:

1 Fully configure an initial template router to the general requirements of the remote installations.

Note It is important that this first router is fully and correctly configured as all further router configurations will be based on this one.

2 From a terminal having TFTP access to the router, upload the Config.p and Config.txt files from the router using the TFTP get command.

For example:

```
TFTP -i 97.20.6.52 get config.p
```

This TFTP command uploads the template configuration (Config.p) in binary mode from the template router with IP address 97.20.6.52.

```
TFTP 97.20.6.52 get config.txt
```

Gets the gas pump configuration file from the template router.

3 Edit (or generate) the Config.txt file as necessary for the routers you want to configure.

The commands in the Config.txt file are described in “Command Line and Gas Pump Configuration File Commands”, p. 265.

For example, the main LAN IP address of the router being gas pump configured is changed to 41.20.7.53 using the following commands in the Config.txt file:

```
lan.1
ip address 41.20.7.52 255.255.255.0
```

Example Config.txt files are given in “Example Config.txt Files”, p. 276.

4 Download the Config.p file to the router being gas pump configured using TFTP.

For example, the following command puts the template configuration file in a router being gas pump configured which has the factory default IP address (192.0.2.1):

```
TFTP -i 192.0.2.1 put config.p
```

Note The Express Router is assigned a default IP address when delivered (192.0.2.1 with a Network Mask of 255.255.255.0).

Note Only one Express Router with the default IP address must be connected the LAN used for gas pump configuring routers at any time, unless using a BootP server on the network. This is to avoid IP address conflicts.

5 Download the Config.txt file to the router being gas pump configured using TFTP.

For example, the following command puts the gas pump configuration file in the router being configured which has the factory default IP address (192.0.2.1):

```
TFTP 192.0.2.1 put config.txt
```

6 Upload the Conf-res.txt file from the router being gas pump configured using TFTP.

7 Check for any error messages in Conf-res.txt.

If there are any errors reported in the Conf-res.txt file, correct them and repeat step 5 to 7 until no errors are reported.

Command Line Configuration

Command line configuration

The Express Router has a command line interface facility allowing you to edit the configuration of the router from a command prompt. Command line configuration does not provide complete configuration of the router, but just the basic parameters required to configure an Internet link. From the command line, you can reconfigure:

- basic LAN parameters, such as IP address
- a CSU/DSU port for T1 service
- Frame Relay services and links
- a PPP leased line.

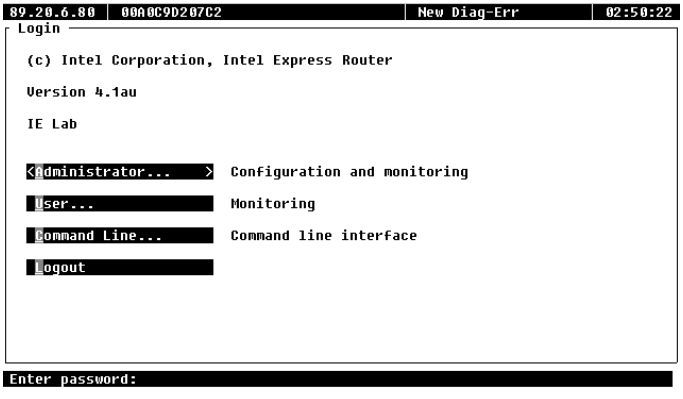
Note You cannot configure the WAN service type on a port or add new links with command line. You must configure these parameters from Intel Device View or Advanced Setup.

For a complete list of commands and their descriptions, see “Command Line and Gas Pump Configuration File Commands”, p. 265.

To access command line configuration

Command line configuration of the router requires that you have a link to Local Management on the router. To access command line interface of Local Management:

- Start any Telnet session to the router.
- Connect a PC or VT100 compatible terminal to the console port of the router. See“Connecting the Console Port to a VT100-compatible Terminal or PC”, p. 30 of Chapter 2.



Note For details on accessing Local Management, see Chapter 4, “Introduction to Local Management”, p. 81.

- To enter command line configuration, select the `Command line` option.

Command prompt

Upon entering command line configuration, the command prompt is displayed. The command prompt is indicated by the router product code followed by a location indicator in parentheses, then the “#” symbol.

Example: `ER9535(config)#`

Command line structure

The command line is structured in a tree-like hierarchy having a root with different sublevels, depending on the router. The commands available at a given prompt depend on your location in the tree.

Command Line and Gas Pump Configuration File Commands

Notes on command syntax and structure

The following syntax is used for gas pump file (Config.txt) and command line configuration of the router:

- An `.x` extension to indicate the port or link index number must be entered. The index number assigned to the port or link can be obtained by viewing the `context.txt` file.
- A parameter within [ ] indicates that it is an option.
- A parameter within < > indicates a user-defined valued must be entered.
- Parameters separated by | indicate a set of choices.
- Commands are not case sensitive (passwords and user names are).
- The space between commands and parameters may contain any number of spaces and tab characters.
- Empty lines are ignored.

- Lines starting with the character "#"will be ignored and can be used to make comments in the Config.txt file.
- Commands must not exceed 100 characters.

The Gas Pump Configuration file (config.txt) must not exceed 4 kilobytes.

Global commands

The following table lists all global commands that can be used anywhere in a gas pump configuration file (Config.txt) or from command line access to the router:

Command	Description
`exit or quit`	To go back one level of the tree or quit the command line if at the Root level.
`root`	Switch to the root directory.
`lan.x`	Switch to the LAN configuration tree for LAN port indicated.
`csu.x`	Switch to the CSU/DSU configuration tree for the port.
`ppp.x`	Switch to the port configuration tree for a PPP leased line, where `x` is the index number of the port. (This command can only be used if the router is configured for leased line operation.)
`frport.x`	Switch to the port configuration tree for Frame Relay services. (This command can only be used if the router is configured for Frame Relay operation.)
`frlink.x`	Switch to a Frame Relay link configuration tree. (This command can only be used if the router is configured for Frame Relay operation.)
`save to flash`	Save the new configuration to flash memory in the router as the permanent configuration. This command must be included to ensure that the new configuration is available following a reset of the router.
`reset`	Reboot the router.

Root commands

The following commands can be used from the root of the command line configuration, indicated by `(config)` in the command prompt, or a gas pump configuration file (Config.txt).

Command	Description
`root`	Switch to the root directory. Must be done before the following commands are valid.
`name` <router name>	Assign a name to the router for management purposes.
`no name`	No name is assigned to the router.
`location` <router location>	Describe the location of the router.
`no location`	No location described.
`admin password` <password>	Administrator password required for configuration and management access to the router.
`no admin password`	No administrator password required for configuration, management and command line access.
`user password <password>`	User password required for management access to the router.
`no user password`	No user password required for management access.
`license key <alias> <license key>`	Activates a multiple software license. <license key> is the key code you receive upon purchase of the feature.

Command	Description
`no license key <license key> <all>`	Deactivates a software license. <license key> is the key code you receive upon purchase of the feature. <all> deactivates all software licenses in the router.
`telnet`	Enables Telnet access to Local Management in the router.
`no telnet`	Disables telnet access to Local Management in the router.
`auth.x [<protocol> <access> <IP address> [community]]`	To define a list of IP addresses that are allowed to access the router using `TFTP`, `Telnet` and `SNMP` and the access privileges (`read-write`, `read-only` or `none`). Read-only access is not valid for the Telnet protocol. Community is only valid if the protocol is SNMP. For example, `Auth.1 TFTP read-write 21.33.4.7` allows full read-write TFTP access to the router from device 21.33.4.7. `Auth.2 SNMP read-only 21.33.4.7 private` allows read-only SNMP management access to the router using the private SNMP community.

LAN commands

To configure the LAN in a gas pump configuration file (config.txt) or from command line access to the router, use these commands. In the config.txt file, these commands can only be entered under the LAN tree. For command line use, LAN configuration must be accessed, as indicated by the presence of `(config-LAN.x)`in the command prompt.

Command	Description
`lan.x`	Switch to the LAN configuration, indicated by `(config-LAN.x)` in the command prompt. Must be done before the following command is valid.
`ip address <IP address> <network mask>`	Sets the main IP address and network mask for the router (factory default IP address is 192.0.2.1). The network mask can either be in the format 255.255.0.0 or alternatively / 16 For example, `21.23.42.7 255.255.0.0` or `21.23.42.7 /16`.
`ip management access`	Enables access to the router for management via the LAN.
`no ip management access`	Management of the router via the LAN is not allowed (disabled).

CSU/DSU port commands

Use the following commands to configure a CSU/DSU port in a gas pump configuration file (config.txt) or from command line access to the router.

Command	Description
`csu.x`	Switch to the CSU/DSU configuration tree indicated by (config-CSU.x) in the command prompt. This must be done before other CSU/DSU commands are available.
`framing ESF|D4`	To set the coding of the frames. `ESF` is most common and should be tried first if the framing cannot be determined from your subscription. Both ends of the WAN link must be configured with the same framing format.
`linecode B8ZS|AMI`	To set how the signal is coded on the line. If `AMI` is selected, the channels speed should be set to 56 Kbps.
`speed 56K|64K`	To set the channel speed. `64K` is most common and recommended. Use `56K` if AMI line coding is used or if directed by your service subscription.
`channel <channel no.> on|off`	To define the use of each channel. The channel number must be between 1 and 24.

PPP leased line commands

Use the following commands to configure a PPP leased line in a gas pump configuration file (Config.txt) or from command line access to the router. In the Config.txt file, the commands must be entered under the PPP tree. For use in command line, PPP configuration must be accessed, as indicated by the presence of (config-PPP.x) in the command prompt.

Command	Description
`ppp.x`	Switch to the PPP leased line configuration tree, indicated by `(config-PPP.x)` in the command prompt. Must be done before the following commands are valid.
`name <link name>`	Assigns a name to the leased line in the router for management purposes.
`no name`	No name is assigned to the leased line link.
`ppp compression`	Enables data compression over the leased line. Compression will be used if it is supported by the router over the leased line.
`no ppp compression`	Data compression is disabled on the leased line.
`ip management access`	Enables access to the router for management over the leased line.
`no ip management access`	Management of the router over the leased line is not allowed (disabled).
`ip numbered <IP address> <network mask>`	Assigns an IP address to the leased line (numbered leased line).
`no number`	No IP address is assigned to the leased line (the leased line is unnumbered).

Command	Description
`ip nat.x <NAT type> <Internal IP address> <Internal Network Mask> <External IP address> [External Network Mask]`	Used to define Network Address Translation (NAT) entries for the router, for example, to convert between public and private IP addresses, multiple and single IP addresses and/or different network sizes. This command can also be used to edit existing NAT entries. The Nat Type can be: `static` a one-to-one translation between an internal and external IP address or network. An internal IP address and Network Mask and an external IP address must be defined. For example: `ip nat.1 static 29.30.6.0 255.255.255.0 92.33.5.0`. `dynamic` translation between IP networks of different sizes. An IP address and Network Mask must be defined for both the internal and external networks. For example: `ip nat.2 dynamic 59.33.0.0 255.255.0.0 12.133.4.0 255.255.255.0`. `singleip` to translate a network IP address to a single IP address using port mapping on the single IP address. This is commonly used on the Internet. An IP address and Network Mask for the internal network and the single external IP address must be defined. For example: `ip nat.3 single 219.130.66.0 255.255.255.0 213.133.45.46`. `singleport` to map a port on a single internal IP address to a specific port number on a single external IP address. This can be used together with Single IP NAT to give access to internal mail servers through the single IP address. For example: `ip nat.4 singleport 43.45.27.23 25 13.33.75.61 25`.

Command	Description
`no ip nat[.x] [entry]`	To delete an IP NAT entry from the table. For example, use no ip nat.3 to delete entry 3 from the nat table. Alternatively use `no ip nat static 29.30.6.0 255.255.255.0 92.33.5.0` to delete the net entry matching static 29.30.6.0 255.255.255.0 92.33.5.0.

Frame Relay Services commands for port configuration

Use the following commands to configure the Frame Relay services (general Frame Relay parameters) on a WAN or CSU/DSU port in a gas pump configuration file (Config.txt) or from command line access to the router.

Command	Description
`frport.x`	Switch to the Frame Relay port configuration tree, indicated by (config-FRPORT.x) in the command prompt. Must be done before the following commands are valid.
`lmi type <type>`	Sets the correct Frame Relay LMI (also known as DLCMI) type being connected to. This can be: `Auto` the router will try to automatically detect the correct Frame Relay switch type and links (DLCIs) in your subscription and default routing will applied—see “Router Factory Default Setup”, p. 21. `annex-A` ITU-T Q.933 `annex-D` ANSI T1.617 `lmi` Cisco§ compatible `none` for connecting the router back-to-back for test purposes.

Frame Relay link commands

Use the following commands to configure a Frame Relay link in a gas pump configuration file (Config.txt) or from command line access to the router:

Command	Description
`frlink.x`	Switch to a Frame Relay link configuration tree, indicated by (config-FRLINK.x) in the command prompt. Must be done before the following commands are valid.
`name <link name>`	Assigns a name to the Frame Relay link in the router for management purposes.
`no name`	No name assigned to the link.
`dlci <number>`	Set the Frame Relay DLCI number for this link from your subscription Must be between 16-991. For example: `dlci 44` to set the DLCI number for the link to 44.
`fr compression`	Enables data compression over the Frame Relay link. Compression will be used if it is supported by the device over the link.
`no fr compression`	Data compression is disabled on the link.
`ip management access`	Enables access to the router for management over the Frame Relay link.
`no ip management access`	Management of the router over the Frame Relay link is not allowed (disabled).
`ip numbered <IP address> <network mask>`	Assigns an IP address to the link.
`no number`	No IP address is assigned to the Frame Relay link (the link is unnumbered).

Command	Description
`ip nat[.x] <NAT type> <Internal IP address> <Internal Network Mask> <External IP address> [External Network Mask]`	Used to define Network Address Translation (NAT) entries for the router, for example, to convert between public and private IP addresses, multiple and single IP addresses and/or different network sizes.This command can also be used to edit existing NAT entries. The Nat Type can be: `static` for one-to-one translation between an internal and external IP address or network. An internal IP address and Network Mask and an external IP address must be defined. For example: `ip nat.1 static 29.30.6.0 255.255.255.0 92.33.5.0`. `dynamic` for translation between IP networks of different sizes. An IP address and Network Mask must be defined for both the internal and external networks. For example: `ip nat.2 dynamic 59.33.0.0 255.255.0.0 12.133.4.0 255.255.255.0`. `singleip` to translate a network IP address to a single IP address using port mapping on the single IP address. This is commonly used on the Internet. An IP address and Network Mask for the internal network and the single external IP address must be defined. For example: `ip nat.3 single 219.130.66.0 255.255.255.0 213.133.45.46`. `singleport` to map a port on a single internal IP address to a specific port number on a single external IP address. This can be used together with Single IP NAT to give access to internal mail servers through the single IP address. For example: `ip nat.4 singleport 43.45.27.23 25 13.33.75.61 25`.

Command	Description
`no ip nat[.x] [entry]`	To delete an IP NAT entry from the table. For example, no ip nat.3 to delete entry 3 from the NAT table. Alternatively use `no ip nat static 29.30.6.0 255.255.255.0 92.33.5.0` to delete the net entry matching static 29.30.6.0 255.255.255.0 92.33.5.0.

Example Config.txt Files

Introduction

The following are examples of config.txt files used for gas pump configuration of the router. The information provided along the left side of the page is for explanatory purposes. The center of the page shows how the information appears in the config.txt file.

Example Config.txt File for a PPP Leased Line Link to the Internet from a CSU/DSU Port

```
# Root commands:
```

Router name

```
name                Internet Router
```

Router location

```
location            Room 302
```

Administrator password required

```
admin password      elephant
```

Passwords for User and TFTP access not required

```
no user password
no tftp password
```

Allow Telnet access

```
telnet

# LAN commands
```

Switch to the LAN configuration tree	lan.1	
Set the main router IP address and subnet mask	ip address	89.20.6.33 255.255.0.0
Allow management access from the LAN	ip management access	
Switch to the CSU/DSU configuration tree	csu.1	
Set the line coding	linecoding	B8ZS
Set the channel speed	speed	64K
Set the framing	framing	ESF
	# Setup leased line parameters.	
Switch to the leased line configuration tree	ppp.1	
Assign a name to the link	name	Internet
Setup CHAP to authenticate this router to the ISP	ppp auth local	chap/pap tp176397 In67JXnK
Authentication is not required for access to this router over the link	no ppp auth remote	
Allow PPP compression if supported (negotiated)	ppp compression	
Do not allow access to the router for management via the ISDN link	no ip management access	

An IP address is not assigned to the link	no ip numbered	
Network Address Translation between the LAN and a single external IP address 194.73.23.26	ip nat.1	singleip 0.0.0.0 0.0.0.0 194.73.23.26
	# Save the configuration to flash memory	
Save the new configuration to flash memory	save to flash	

Example Config.txt File for a Frame Relay Link to the Internet from a WAN Port

	# Root commands
Router name	name Internet Router
Router location	location Room 302
Administrator password required	admin password elephant
Passwords for User and TFTP access not required	no user password no tftp password
Allow Telnet access	telnet
	# LAN commands
Switch to the LAN configuration tree	lan.1
Set the main router IP address and subnet mask	ip address 89.20.6.33 255.255.0.0
Allow management access from the LAN	ip management access
	# Setup general Frame Relay parameters
Switch to the Frame Relay port configuration tree	frport.1
Select the Frame Relay Switch (LMI) type	lmi type annex-d
	# Setup Frame Relay link parameters.

Switch to the Frame Relay link configuration tree	frlink.1
Assign a name to the Frame Relay link	name Internet
Set the DLCI for the link	dlci 57
Setup CHAP to authenticate this router to the ISP	ppp auth local chap/pap tp176397 In67JXnK
Authentication is not required for access to this router over the link	no ppp auth remote
Allow Frame Relay compression if supported (negotiated)	fr compression
Do not allow access to the router for management via the ISDN link	no ip management access
An IP address is assigned to the Frame Relay link	ip numbered 124.35.13.1 255.255.255.0
Network Address Translation between the LAN and a range or external (Internet) IP addresses	ip nat.1 static 89.20.6.52 255.255.255.255 124.35.13.2 ip nat.2 dynamic 89.20.0.0 255.255.0.0 124.35.13.0 255.255.255.0
	# Save the configuration to flash memory
Switch to the root of the configuration tree	root
Save the new configuration to flash memory	save to flash

13 Troubleshooting

Introduction

This chapter provides guidance in the event the Express Router is not operating satisfactory. It describes the troubleshooting tools available and how to use them to isolate and correct problems in the router.

The chapter addresses some typical problems that can occur in the router, providing possible causes and recommended corrective actions. The majority of the troubleshooting procedures are based on the use of Intel Device View, however there are diagnostic features available from Local Management as well.

Troubleshooting Tools

Tools available

The tools available for troubleshooting on the router are:

The LED indicators

The LEDs give a general status of the router and specific router ports. The LEDs are described in “LED Descriptions”, p. 5.

Intel Device View

Intel Device View offers extensive information about the performance and the status of the router and is considered the main tool for troubleshooting.

Intel Device View provides these useful features:

- Diagnostics

  Diagnostics automatically display potential problems and provide possible causes and solutions.

- Autofix

  The Diagnostics has an extensive autofix feature which automatically corrects errors when you select the option.

- Full SNMP monitoring of the router, including a list of the SNMP traps generated when the router detects a potential problem.
- Router configuration to your installation requirements.
- Logs system events—both normal and abnormal events.
- Recovery Mode Manager to gain control of the router if it is rendered inoperable.
- TFTP Server to download firmware to the router.

Local Management

Local Management has an extensive diagnostic system that provides a description of current problems and suggests corrective actions.

Troubleshooting Procedure

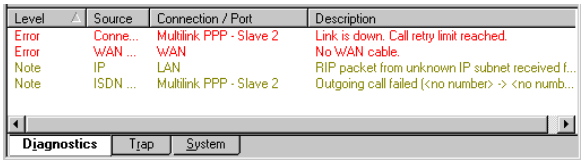
Isolating the Problem

To isolate the problem using Intel Device View

If the router fails to forward data for any reason, use the following procedure to isolate the problem:

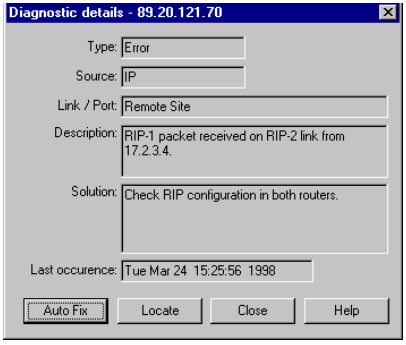
1 Check the LEDs.
The LEDs provide immediate information about the status of the router and the status of the LAN and WAN ports on the router.
Check the LEDs on the router itself or in Intel Device View. The functions of the LEDs are described in “LED Descriptions”, p. 5. See the on-line help for a key to the LEDs displayed in Intel Device View.

2 In Intel Device View, check for messages in the `Diagnostic` window.



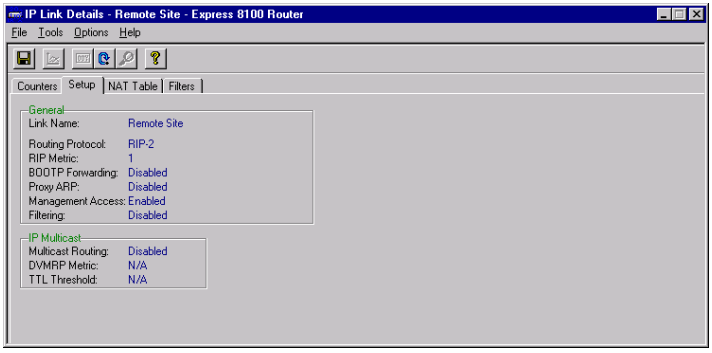
The diagnostic tool automatically detects potential problems with the router and provides possible causes and solutions.

Double-click on the diagnostic message to get a description of the problem and possible corrective actions in priority order.



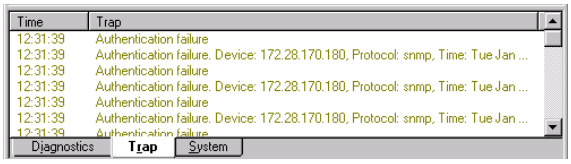
Select `Auto Fix` to automatically correct the problem. This function is not available for all problems.

Select `Locate` to display the counter or the layer in Intel Device View Explorer relevant to the problem as appropriate.



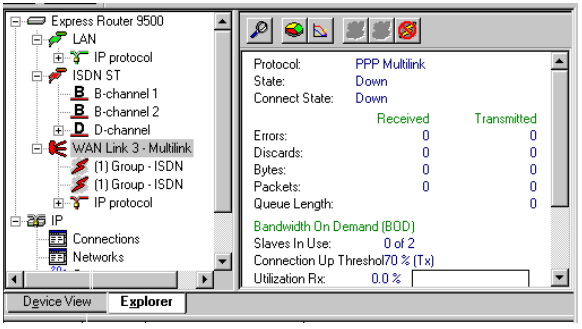
In Explore View select `Details` to display the counters and setup relevant to the problem.

3 To check the SNMP traps select the `Trap` tab.



SNMP traps provide current status information about the router and are generated for all major router events. For historical information, check the log from the router (step 5 in this procedure). The PC running Intel Device View for Windows must be set up as an SNMP Traps destination for the router before traps are displayed.

4 Use Intel Device View Explorer to try to locate the problem.

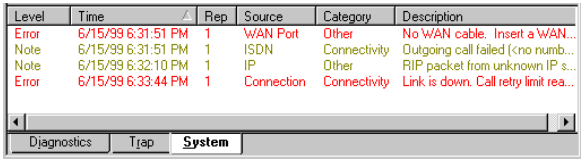


If a link is operational (up), it is displayed in green. If a link or port is not operational (down), it is displayed in red. An X.25 link in timecut is displayed in yellow.

This will help you find the source of the problem whether it is a port, a link on the port or a network protocol problem.

5 Check for any relevant messages in the System Log.

On the Intel Device View select the `System` tab.



The log records all events that occur in the router and provides valuable information. The log records a variety of events such as when WAN links are brought up or down, failed calls, spanning tree bridging topology changes, system changes, unexpected events (for example, WAN links failing to establish, routing protocol problems), configuration errors and so on.

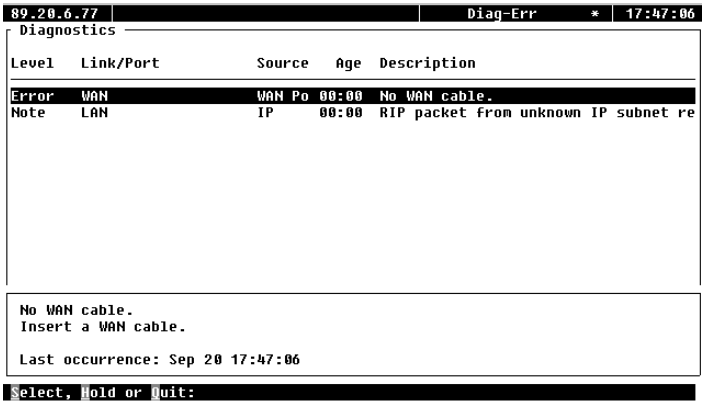
6 If the problem can still not be resolved satisfactorily, use the Monitoring menu and the Explorer within Intel Device View to access information on the problem area (link or protocol). The Monitoring menu and the Explorer offer extensive information on the performance and the status of the LAN and WAN ports on the router, the routing protocols (IP and IPX) and bridging service.

Use the on-line help within the monitoring screens for information contained in the monitoring screens, such as counters and statistics.

Using Local Management diagnostics

To troubleshoot a problem using Local Management:

1. Access Local Management on the router.
2. From the Local Management main display, select `Troubleshooting`.



The router diagnostics is displayed.

3. To view a description and suggested corrective action for an event, select the event and press <`Enter`>.

Typical Problems and Causes

Typical Problems that could be encountered

This section gives some examples of typical problems encountered during the installation and configuration of the Express Router, and there possible cause. Configuration problems, defective cables and problems communicating with Public Data Network switches are often the cause of router malfunctions. Corrective actions are listed in priority order.

General Problems

After making configuration changes, the router is restarting with the old configuration

Possible cause

If you make changes to the configuration and save them from Device Setup, the changes are active but are only saved to RAM in the router. To save a new configuration as the permanent configuration (the configuration used whenever the router is started up), it must be saved to the flash memory.

Corrective action

If you make changes to the router's configuration and are satisfied with the new configuration, remember to save the changes to the flash memory in the router by selecting `Configuration` > `Save to Flash Memory` in Intel Device View—this menu option is only available if the configuration is different from the permanent configuration stored in flash memory.

The status of the configuration is given in the Information Panel of the Intel Device View.

Console Port and Modem Problems

Modem is not detected on the console port

Possible causes

The following are possible causes for the router failing to detect a modem connected to the `Console` port.

- The console port is not in the `Modem` mode.
- The wrong cable type is being used.
- The console port is configured incorrectly for the modem.
- The default modem initialization string can not be used with your modem.
- The modem is incompatible with the Express Router.
- The router was placed in the Recovery mode and not reset to the previous configuration.

Corrective action

To correct problems with a modem connected to the console port:

1. Check that the console port is in the `Modem` mode.
   - From Intel Device View, use Connection Setup on the console port.
   - From Advanced Setup (Local Management) main display, select `Management` > `Console Port`.
2. Check that the proper modem cable is being used and that physical links are secure.
3. Check that the console port configuration is correct for the modem being used.

   If you are not using a predefined modem profile, verify that the initialization strings are in accordance with the manufacturer's data. When using a custom modem profile, it is recommended that you base the profile on a predefined profile.
4. Run a modem check using a VT100-compatible terminal to verify the router can communicate with the modem.
   - Connect a VT100-compatible terminal or PC (running terminal emulation software) to the modem using the modem cable and any necessary adapters.

- At the screen command prompt, enter the command AT then press Enter.

An OK message sent from the modem should appear on screen. If not, this may indicate an error or improper modem configuration (for example, incorrect DIP switch settings). Refer to the modem manufacturer documentation for details.

Cannot communicate with the router from a terminal connected to the console port

Possible causes

The following are possible causes of communication problems between a VT100-compatible terminal and the router.

- The console port is not in `Console` mode.
- An improper cable is being used.
- The terminal is not VT100-compatible.
- The communication settings of the VT100-compatible terminal are incorrect.

Corrective action

To correct problems associated with a VT100-compatible terminal connected to the console port:

1. Check the physical link and ensure the proper cable is being used.
2. Check that the console port is in the `Modem` mode.
   - From Intel Device View, use Connection Setup on the console port.
   - From Advanced Setup (Local Management) main display, select `Management` > `Console Port`.
3. Check that the communication parameters are set correctly.

   See “Connecting the Console Port to a VT100-compatible Terminal or PC”, p. 30 for details.
4. Check terminal manufacturer data that the terminal is VT100-compatible.

WAN Link Problems

CSU/DSU related errors

Possible causes

The following are possible causes for improper operation of a link(s) on a CSU/DSU port.

- The cable is not connected properly
- The CSU/DSU is configured incorrectly.

Corrective Action

The following troubleshooting steps are recommended in case of problems related to the CSU/DSU.

1 Check for any relevant messages in the `Diagnostics` and `System Log` and for relevant SNMP `Traps`.

Use the Autofix feature of Intel Device View Diagnostics when available to correct any problems.

2 Check that the cables are properly connected.

3 Verify that the CSU/DSU configuration parameters are correct for your T1 service. Use the LEDs to help identify incorrect configuration.

LED	Color	Possible cause...
CSU Status	red	Incorrect framing format
	intermittent orange flashes	Incorrect line coding
CSU Network	orange (CSU Status LED is green)	Incorrect channel speed
		Incorrect data inversion
		Incorrect channel selection

Leased line link will not start up

Possible causes

The following are possible causes for a leased line failure on either of the routers over the leased line:

- The wrong cable type is being used.
- The cable is not properly connected.
- The PPP protocol is not used in the remote router.
- Device authentication over the link using the Challenge Handshake Authentication Protocol (CHAP) or the Password Authentication Protocol (PAP) is incorrectly configured.
- PPP protocol conflict.
- The modem configuration is incorrect.
- The link configuration in the remote router is incorrect.

Corrective action

To correct a PPP leased line failure:

1. Check for any relevant messages in the `Diagnostics` and `System Log` and for relevant SNMP `Traps`.
2. Check the cables are connected correctly.
3. Check you are using the correct cable type.

   The connect cables available for the Express Router are listed in Chapter 2 “Optional product parts”, p. 24.
4. Check the WAN protocol in the routers over the leased line is PPP. Use Connection Setup in Intel Device View. See “Configuring a WAN Port (WAN, CSU/DSU, HDSL2, and Console port)”, p. 60.
5. If CHAP or PAP is in use over the link, check the Local IDs, the Remote IDs (CHAP only) and the associated passwords as necessary. Use Connection Setup in Intel Device View. See “Adding and Editing Remote Connections”, p. 61.
6. Check that the modem connecting the router to the Public Data Network (PDN) is setup correctly. Refer to the modem manufacturer documentation.

Data compression is configured but does not work

Possible cause

Data compression is not enabled or supported in the remote router.

Corrective action

To correct data compression failure:

1. Check for any relevant messages in the `Diagnostics` and `System Log` and for relevant SNMP `Traps`.
2. Check the state of the data compression.
   - From Intel Device View Explorer, select the link and click the `Details` icon .
   - Open the `Compression` folder.

Abnormal X.25 SVC behavior

Possible cause

The dial-up parameters are different between the routers on either side of the X.25 SVC.

Corrective action

To correct problems with the dial-up (switched) behavior of an X.25 SVC:

1. Check for any relevant messages in the `Diagnostics` and `System Log` and for any relevant SNMP `Traps`. Some dial-up link problems can be fixed automatically. From Intel Device View, click Auto Fix on the Diagnostic details screen.
2. Check that the configuration matches on both routers over the X.25 SVC.

TCP/IP Related Problems

IP routing will not forward data traffic

Possible causes

The following are possible causes for IP routing services failure to forward data traffic:

- IP is not enabled on the link.
- RIP is not enabled on the link.
- The wrong version of RIP is enabled on the link (RIP-1 and RIP-2 are not compatible).
- Triggered RIP is enabled in one router but not in the other.
- A numbered link is defined on one router but not on the other.
- A static route is configured at one end of the link, but is not configured at the other end.
- An incorrect subnet mask is configured.
- IP filters have been established in one or both routers which discard the data traffic or essential network services to route the data traffic (for example, RIP).

Corrective action

To correct IP routing services failure to forward data traffic:

1. Check for any relevant messages in the `Diagnostics` and `System Log` and for relevant SNMP `Traps`.
2. Check the correct version of RIP is enabled on the link(s) and that the IP subnet masks is correct in both routers over the WAN link.
   - From Intel Device View Explorer view, select the IP protocol for the link and click the icon.
   - To check the routing protocol configuration, Open the `Setup` folder.
3. Check if a route to the network is known in the network table, and if the metric to the network is correct.

   From Intel Device View, select Monitoring > IP > Networks.
4. Check that no IP filters are defined which discard the data traffic or essential network services to route the data traffic (for example, RIP).

- From Intel Device View Explorer view, select the IP protocol for the link and click the icon.
- To check the filters configured for the link, open the `Filters` folder.

Note A packet logging feature to captures the information of filtered packets. IP packets matching the filter criteria are recorded in the log for the router.

Equipment will not boot over a WAN link

Possible causes

The following are possible causes for boot failure over a WAN link:

- BootP forwarding is not enabled.
- The RIP metric for the route from the TFTP server to the equipment is too high.
- Max BootP Request Hops in the router is exceeded.
- IP filters are established in one or both routers which discard the BootP or TFTP data traffic or essential network services to route the traffic (for example, RIP).

Corrective action

To correct boot failure over a WAN link:

1. If the Express Router is operating as a remote boot provider, ensure that a static link to the network of the device being booted has been established.
   - From Intel Device View, select `IP` > `Static Route` from the `Configuration` menu and check the static route.
   - From Advanced setup, select `Protocols` > `IP` > `Static Routes` and check the static route.
2. Check if `BootP/DHCP Request Forwarding` is enabled on the router link via which the remote router is attempting to boot (via the static route) in Device Setup.

   From Advanced Setup, select `Protocols` > `IP` > select `link` > `Setup` > `Advanced` and check if `BootP/DHCP Request Forwarding` is enabled.

3 Check the RIP metrics for the route involved.

From Intel Device View, select Monitoring > IP > Networks and determine the metrics for the route. If the sum of the RIP metrics exceeds 15, boot is not possible.

4 Check that the Max Hops Allowed parameter is equal to or greater than the number of hops traversed from the router to the boot server.

In Intel Device View, select Monitoring > IP > Counters and open the BOOTP folder to check the Max Hops Allowed parameter.

5 Check that no IP filters have been defined which are discarding BootP or TFTP traffic (in both routers) or essential network services required for routing the traffic (for example, RIP).

- From Intel Device View, select the IP protocol for the link and click the icon.
- Open the Filters folder to check the filters configured for the link.

Note A packet logging function is also available to capture the information of filtered packets. IP packets matching the filter criteria are recorded in the log for the router.

IPX Related Problems

IPX WAN link will not initialize

Possible causes

The following are possible causes for an IPX WAN link failure to initialize:

- IPX is not enabled on the link.
- The IPX WAN protocol is incorrectly configured.
- There is an incorrect configuration of numbered/unnumbered link.

Corrective action

To correct IPX WAN initialization failure:

1. Check for any relevant messages in the `Diagnostics` and `System Log` and for relevant SNMP `Traps`.
2. Check that both routers use the same numbered or unnumbered links configuration.
   - From Intel Device View, select the `IPX protocol` for the link in Intel Device View Explorer. Click the and then click the link.
   - Open the `Setup` folder to check if a `Net Number` is assigned to the link.
3. Check that the IPX WAN protocol is enabled or disabled in both the routers over the Wan link.

   From Advanced Setup, select `Protocols` > `IPX` > select `link` > `Advanced` and check if the IPX WAN protocol is enabled.

IPX routing will not forward data traffic

Possible causes

The following are possible causes for an IPX routing services failure:

- The Frame Type configured on the LAN port does not match the Frame Type in use on the LAN.
- SAP and RIP filters are incorrectly defined.

Corrective action

To correct IPX routing services failure:

1. Check for any relevant messages in the `Diagnostics` and `System Log` and for relevant SNMP `Traps`.
2. If the Novell Server is on the same LAN as the router, check that the frame type configured for the router is the same as is used by the Novell server.
   - From Intel Device View Explorer, select the IPX protocol for the link and select the icon.
   - Open the `Setup` folder to check that the correct Frame Type is configured for the link.

3 Check RIP and SAP filters defined do not filter out essential information to the router.

From Advanced Setup, select `Protocols` > `IPX` > select `link` > `Advanced`. From this screen, access the RIP and SAP Tx and Rx filters.

WAN Bridging Related Problems

Duplicated frames are seen on a network segment

Possible cause

The Spanning Tree Algorithm is not enabled on all links.

Corrective action

Check that the Spanning Tree Algorithm is enabled on all links.

For each link, select the `Bridge protocol` in Intel Device View Explorer. Select the and then open the `Setup` folder to check if Spanning Tree is enabled on the link.

Unable to bridge IPX data traffic

Possible causes

The following are possible causes for IPX data traffic not being bridged:

- IPX routing is not disabled—IPX routing must be completely disabled before IPX data will be bridged. In the Express Router, IPX routing services must be configured for a particular Ethernet frame type (SNAP, TYPE, 802.2 or 802.3). All other IPX Ethernet frames types will be bridged if bridging services are enabled.
- Bridging is not enabled for the router or is not configured on all the necessary links

Corrective action

To correct Bridging services failure to forward IPX data traffic:

1. Check that IPX routing is disabled.

   From Intel Device View Explorer, if the `IPX protocol` is not displayed on the network protocol layer then it is not enabled for the router or configured on the link.

2. Check that Bridging is enabled on all the relevant links.

   From Intel Device View Explorer, if the `Bridge protocol` is not displayed on the network protocol layer then it is not enabled for the router or configured on the link.

Unable to bridge IP data traffic

Possible causes

The following are possible causes for IP data traffic not being bridged:

- IP routing is not disabled—IP routing must be completely disabled before IP data will be bridged.
- Bridging is not enabled for the router or is not configured on all the necessary links.

Corrective action

To correct Bridging services not forwarding IP data traffic:

1. Check that IP routing is disabled.

   From Intel Device View Explorer, if the `IP protocol` is not displayed on the network protocol layer for the LAN link then it is not enabled for the router.

2. Check that Bridging is enabled on all the relevant links.

   From Intel Device View Explorer, if the `Bridge protocol` is not displayed on the network protocol layer (`IP protocol` and `IPX protocol` will also be displayed if configured) then it is not enabled for the router or configured on the link.

Long delays for bridged data traffic

Possible causes

Long delays in bridged traffic can be caused by topology changes in the Spanning Tree bridged network. When a topology change is taking place, at least two `Forwarding Delays` must elapse before a link can start forwarding traffic. If the Spanning Tree is unstable, frequent topology changes can cause long delays. Instabilities in the

Spanning Tree are often caused by links going down and also by timouts of the messages transmitted via Spanning Tree BPDU frames. Such BPDU timeouts can be caused by:

- The bridge which is assigned as Root Bridge of the spanning tree is too far from the center of the tree.
- The `Max Age` parameter for the Root Bridge is too low.
- The maximum of 7 network segment hops (defined by the Spanning Tree Algorithm) is exceeded.

Corrective action

To correct long delays with bridging services:

1. Check for any relevant messages in the `Diagnostics` and `System Log` and for any relevant SNMP `Traps`.
2. Check if any of the WAN links which are part of the Spanning Tree are going down frequently.
   Refer to the “General Problems”, p. 287, for guidance on specific WAN link problems.
   Refer to “Troubleshooting Procedure”, p. 282 for a more general approach to isolating the problem.
3. Configure a bridge that is more central to the bridged network as the Root Bridge.
4. Increase the value of the Max Age timer in the Root Bridge of the Spanning Tree.
5. If the 7-hop limit is exceeded, divide the bridged network into two separate Spanning Trees. Use a Non-Spanning Tree between the two separated Spanning Trees.

14 Recovery Mode

Overview

Recovery Mode

The Recovery Mode feature allows you to regain control and restore operation of the router in the event it fails. This can be caused by, for example, a mismatched router configuration or corrupted firmware. The Recovery Mode provides a way to get the router up and running again without the need to reconfigure, in most cases.

The router is placed in the Recovery Mode using the recovery button on the back of the router. In the Recovery Mode, you can gain control of the router from:

- Intel Device View using the Recovery Mode Manager, or
- a VT100-compatible terminal connected to the console port of the router.

When to use the Recovery Mode

Use the Recovery Mode in these situations:

- The router cannot be started using the firmware and configuration stored in flash memory. The firmware is crashed or corrupted.
- You cannot manage the device from Intel Device View.
- You forgot the IP address of the router.

- The device is on a new network and the IP address is invalid.
- You cannot gain access to Local Management from the console port.

When in Recovery Mode the router is not operational, only simple commands can be sent to the router from the Recovery Manager of Intel Device View or from a command line interface from the console port.

Automatic Recovery Mode

The router is automatically placed in Recovery Mode when the router does not detect a valid firmware during start-up or the firmware is corrupted during operation.

Network Boot Process using the Recovery Mode

Boot firmware location

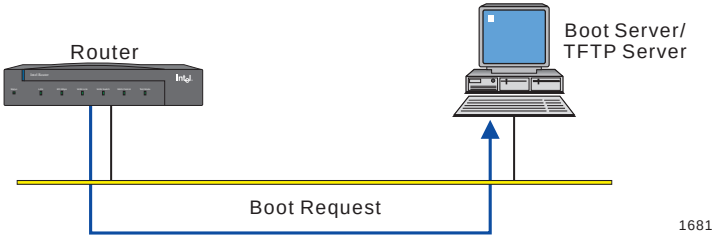
The firmware and configuration of the router is stored in router's internal flash memory (FlashPROM). The router boots from the flash memory.

You can use a network boot server and a TFTP server to automatically load firmware and boot the router if the router can not start up using the firmware in the flash memory. To do this, the router must be in Recovery Mode.

Network boot process

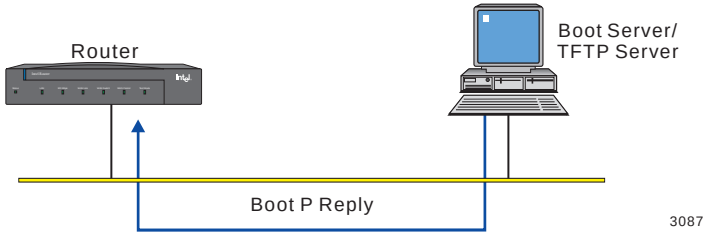
This describes a network boot process.

1. When in Recovery Mode, the router sends a BootP request over the network.

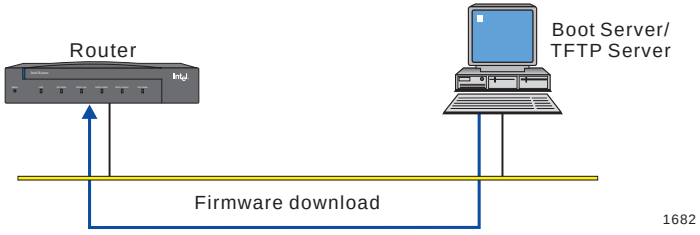


The boot request contains the router's MAC address.

2. If a boot server recognizes the router from the BootP request, it sends a BootP reply to the router.



3. The router receives the BootP reply and initiates a TFTP file transfer to download the firmware and IP address from the TFTP server to the router.



Using Recovery Mode Manager in Intel Device View

Recovery Mode Manager

The Recovery Mode Manager in Intel Device View provides an easy way to gain control of a router on your LAN if you know its MAC address.

You need physical access to the router to enter into the Recovery Mode.

Note If the router has an invalid IP address, select `Manage` form the `Device` menu or and enter the MAC address for the router. The MAC address is printed on the label next to the LAN port on the router.

To use the Recovery Mode Manager

To use Intel Device View Recovery Mode Manager to gain control and operation of a router:

1 Enter Recovery Mode:

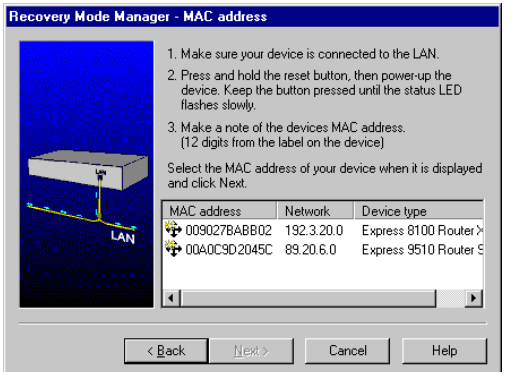
Use a pointed tool, such as the tip of a pen or paper clip, and press the recovery button on the back of the router.

After a few seconds, the Status LED blinks orange which indicates the router is in Recovery Mode.

2 From the `Tools` menu Intel Device View, click `Recovery Manager`.

Click `Next` to continue.

3 When the MAC address of the router appears on the screen, select it and click `Next`.



Follow the on-screen instructions to complete the recovery.

Using the Recovery Mode from the Console Port

Recovery Mode from the console port

Connect a VT100 compatible terminal to the console port when the router is in the Recovery Mode to recover operation of the router from a command-line interface. The Recovery Mode command-line interface allows you to:

- run the router firmware from its flash memory.
- download firmware from a BOOTP or TFTP server.
- reboot the router, similar to a power up.
- display hardware and firmware information.

To recover the router from the console port

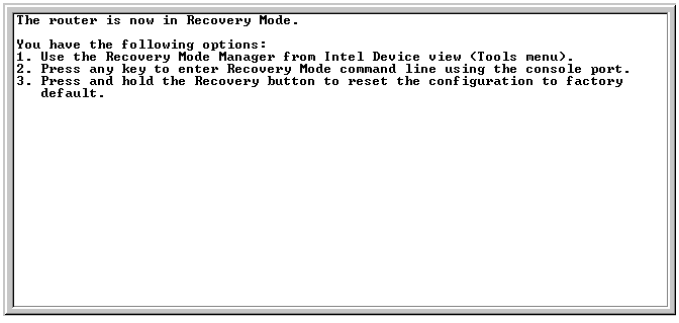
Follow this procedure to use Recovery Mode from the console port of router to regain its control and operation.

1 Connect a VT100-compatible terminal to the console port and run the terminal emulation program.

See “Connecting the Console Port to a VT100-compatible Terminal or PC”, p. 30 for details.

2 Enter the Recovery Mode as follows:

Use a pointed tool, such as the tip of a pen, and press the recovery button on the back of the router. After a few seconds, the Status LED blinks orange which indicates the router is in Recovery Mode.



3 Press any key to enter the Recovery Mode command line interface. This is indicated by the `Recovery>` prompt.

4 Enter the necessary commands at the screen prompt. Type Help for a list of available commands.

Recovery Mode commands

These commands are available from the command prompt in the Recovery Mode.

`QUIT`

Exit the Recovery mode and restart the router.

`BOOTP [filename]`

Initiates a BOOTP request from the LAN interface for a firmware download using TFTP protocol.
[filename] is optional and is the path and name of the firmware file on the TFTP server.

`DUMP <addr>`

Displays the contents of the memory from the hex address <addr>.

`HELP`

Displays the commands.

`INFO`

Displays the router hardware including the MAC address.

`RESET [cold]`

Performs a reboot of the router. The cold option starts the router as if it was a turned on.

`RUN [DEFPARM]`

Runs the firmware and configuration in the FlashPROM. Enter `DEFPARM` to set the router to the factory default configuration.

`UNPROTECT`

Removes protection from the Boot sector to allow for the BootPROM loading.

Warning This is for internal use and not recommended.

`SETMAC <mac-address>`

Defines a new MAC address for the router.

Warning This is for internal use and not recommended.

`TFTP <filename> <ownIP> <tftpIP> [gwIP]`

Loads the router's firmware from a specified TFTP server via the LAN interface, where:

- <filename> is the name of file containing the firmware.
- <ownIP> is the IP address of the router.
- <tftpIP> is the IP address of the TFTP server.
- [gwIP] is the IP address of intermediate gateway, if any.

Resetting to Factory Default Configuration Using the Recovery Button

To set the router to the factory default configuration

The Recovery button allows you to reset your Express Router to the factory default configuration. To set the router to the factory default:

Note The current router configuration is lost when it is reset to the factory default setting.

1. Using a pointed tool, press the recovery button on the back of the Express Router.

   After a few seconds, the Status LED will blink orange. The router is now in Recovery Mode.

2. Press and hold the Recovery button again until the LEDs begin to blink in sequence.

   When the Status LED blinks green, the router is set to the factory default configuration.

A Limited Hardware Warranty

Intel warrants to the original owner that the hardware product delivered in this package will be free from defects in material and workmanship for one (1) year following the latter of: (i) the date of purchase only if you register by returning the registration card as indicated thereon with proof of purchase; or (ii) the date of manufacture; or (iii) the registration date if by electronic means provided such registration occurs within 30 days from purchase. This warranty does not cover the product if it is damaged in the process of being installed. Intel recommends that you have the company from whom you purchased this product install the product.

INTEL RESERVES THE RIGHT TO FILL YOUR ORDER WITH A PRODUCT CONTAINING NEW OR REMANUFACTURED COMPONENTS. THE ABOVE WARRANTY IS IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

This warranty does not cover replacement of products damaged by abuse, accident, misuse, neglect, alteration, repair, disaster, improper installation or improper testing. If the product is found to be otherwise defective, Intel, at its option, will replace or repair the product at no charge except as set forth below, provided that you deliver the product along with a return material authorization (RMA) number either to the company from whom you purchased it or to Intel (North America only). If you ship the product, you must assume the risk of damage or loss in transit. You must use the original container (or the equivalent) and pay the shipping charge. Intel may replace or repair the product with either new or remanufactured product or parts, and the returned product becomes Intel's property. Intel warrants the repaired or replaced product to be free from defects in material and workmanship for a period of the greater of: (i) ninety (90) days from the return shipping date; or (ii) the period of time remaining on the original one (1) year warranty.

This warranty gives you specific legal rights and you may have other rights which vary from state to state. All parts or components contained in this product are covered by Intel's limited warranty for this product; the product may contain fully tested, recycled parts, warranted as if new. For warranty information call one of the numbers below.

Returning a Defective Product (RMA)

Before returning any product, contact an Intel Customer Support Group and obtain an RMA number by calling:

North America only:	1-916-377-7000
Europe Only:	See RMA information under "Limited Hardware Warranty (Europe Only)"
Other locations:	Return the product to the place of purchase for a refund or replacement.

If the Customer Support Group verifies that the product is defective, they will have the Return Material Authorization Department issue you an RMA number to place on the outer package of the product. Intel cannot accept any product without an RMA number on the package.

LIMITATION OF LIABILITY AND REMEDIES

INTEL SHALL HAVE NO LIABILITY FOR ANY INDIRECT OR SPECULATIVE DAMAGES (INCLUDING, WITHOUT LIMITING THE FOREGOING, CONSEQUENTIAL, INCIDENTAL AND SPECIAL DAMAGES) ARISING FROM THE USE OF OR INABILITY TO USE THIS PRODUCT, WHETHER ARISING OUT OF CONTRACT, NEGLIGENCE, TORT, OR UNDER ANY WARRANTY, IRRESPECTIVE OF WHETHER INTEL HAS ADVANCE NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES, INCLUDING, BUT NOT LIMITED TO LOSS OF USE, BUSINESS INTERRUPTIONS, AND LOSS OF PROFITS, NOTWITHSTANDING THE FOREGOING, INTEL'S TOTAL LIABILITY FOR ALL CLAIMS UNDER THIS AGREEMENT SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THESE LIMITATIONS ON POTENTIAL LIABILITIES WERE AN ESSENTIAL ELEMENT IN SETTING THE PRODUCT PRICE. INTEL NEITHER ASSUMES NOR AUTHORIZES ANYONE TO ASSUME FOR IT ANY OTHER LIABILITIES.

Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions may not apply to you.

Software provided with the hardware product is not covered under the hardware warranty described above. See the applicable software license agreement which shipped with the hardware product for details on any software warranty.

Limited Hardware Warranty (Europe only)

Intel Corporation (UK) Ltd. for customers within the UK and Intel International Ltd. (Intel Corporation (UK) Ltd. and Intel International Ltd. hereinafter referred to collectively as "Intel") for customers within Europe outside of the UK warrants to the original owner that the hardware product delivered in this package will be free from defects in material and workmanship for one (1) year following the latter of: (i) the date of purchase only if you register by returning the registration card as indicated thereon with proof of purchase; or (ii) the date of manufacture; or (iii) the registration date if by electronic means provided such registration occurs within 30 days from purchase. This warranty does not cover the product if it is damaged in the process of being installed. Intel recommends that you have the company from whom you purchased this product install the product.

INTEL RESERVES THE RIGHT TO FILL YOUR ORDER WITH A PRODUCT CONTAINING NEW OR REMANUFACTURED COMPONENTS. THE ABOVE WARRANTY IS IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

This warranty does not cover replacement of products damaged by abuse, accident, misuse, neglect, alteration, repair, disaster, improper installation or improper testing. If the product is found to be otherwise defective, Intel, at its option, will replace or repair the product at no charge except as set forth below, provided that you deliver the product along with a return material authorization (RMA) number either to the company from whom you purchased it or to Intel. If you ship the product, you must assume the risk of damage or loss in transit. You must use the original container (or the equivalent) and pay the shipping charge. Intel may replace or repair the product with either new or remanufactured product or parts, and the returned product becomes Intel's property. Intel warrants the repaired or replaced product to be free from defects in material and workmanship for a period of the greater of: (i) ninety (90) days from the return shipping date; or (ii) the period of time remaining on the original one (1) year warranty.

This warranty gives you specific legal rights and you may have other rights which vary from state to state. All parts or components contained in this product are covered by Intel's limited warranty for this product; the product may contain fully tested, recycled parts, warranted as if new.

Returning a Defective Product (RMA)
Before returning any product, contact an Intel Customer Support Group and obtain an RMA number by calling one of the following numbers for the applicable language in which you require support:

France	+33 (0) 1 41 91 85 29
Germany	+49 (0) 69 9509 6099
Italy	+39 (0) 2 696 33276
United Kingdom	(+44) (0) 870 607 2439

If the Customer Support Group verifies that the product is defective, they will have the Return Material Authorization Department issue you an RMA number to place on the outer package of the product. Intel cannot accept any product without an RMA number on the package.

LIMITATION OF LIABILITY AND REMEDIES

INTEL SHALL HAVE NO LIABILITY FOR ANY INDIRECT OR SPECULATIVE DAMAGES (INCLUDING, WITHOUT LIMITING THE FOREGOING, CONSEQUENTIAL, INCIDENTAL AND SPECIAL DAMAGES) ARISING FROM THE USE OF OR INABILITY TO USE THIS PRODUCT, WHETHER ARISING OUT OF CONTRACT, NEGLIGENCE, TORT, OR UNDER ANY WARRANTY, IRRESPECTIVE OF WHETHER INTEL HAS ADVANCE NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES, INCLUDING, BUT NOT LIMITED TO LOSS OF USE, BUSINESS INTERRUPTIONS, AND LOSS OF PROFITS, NOTWITHSTANDING THE FOREGOING, INTEL'S TOTAL LIABILITY FOR ALL CLAIMS UNDER THIS AGREEMENT SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THESE LIMITATIONS ON POTENTIAL LIABILITIES WERE AN ESSENTIAL ELEMENT IN SETTING THE PRODUCT PRICE. INTEL NEITHER ASSUMES NOR AUTHORIZES ANYONE TO ASSUME FOR IT ANY OTHER LIABILITIES.

Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions may not apply to you.

Software provided with the hardware product is not covered under the hardware warranty described above. See the applicable software license agreement which shipped with the hardware product for details on any software warranty.

This Agreement shall be governed by the laws of England and the courts of England shall have exclusive jurisdiction of any dispute arising hereunder.

Federal Communications Commission (FCC) Statement

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.

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user's authority to operate this equipment.

Manufacturer Declaration

Intel declares that the Express Router complies with the EU Directive 89/336/EEC, using the EMC standards EN55022 and EN55024. These products also meet EU Directives 73/23/EEC and 93/68/ and are certified by DEMKO to be compliant with EN60950/A1/A2/A3/A4 and by UL to be compliant with UL 1950. These products have been tested and verified to meet CISPR 22 Class A requirements and FCC Part 15 Class A.

WARNING

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.**WARNING**

警告使用者 ：
這是甲類的資訊產品， 在居住的環境中使用時，
可能會造成射頻干擾， 在這種情況下，使用者會
被要求採取某些適當的對策。

The system is designed to operate in a typical office environment. Choose a site that is:

- Clean and free of airborne particles (other than normal room dust).
- Well ventilated and away from sources of heat including direct sunlight.
- Away from sources of vibration or physical shock.
- Isolated from strong electromagnetic fields produced by electrical devices.
- In regions that are susceptible to electrical storms, we recommend you plug your system into a surge suppressor and disconnect telecommunication lines to your modem during an electrical storm.
- Provided with a properly grounded wall outlet.

Do not attempt to modify or use the supplied AC power cord if it is not the exact type required.

Ensure that the system is disconnected from its power source and from all telecommunications links, networks, or modems lines whenever the chassis cover is to be removed. Do not operate the system with the cover removed.

AVERTISSEMENT

Le système a été conçu pour fonctionner dans un cadre de travail normal. L'emplacement choisi doit Ítre:

- Propre et dépourvu de poussière en suspension (sauf la poussière normale).
- Bien aèrè et loin des sources de chaleur, y compris du soleil direct.

- A l'abri des chocs et des sources de ibrations.
- Isolé de forts champs magnétiques géenérés par des appareils électriques.
- Dans les régions sujettes aux orages magnétiques il est recomandé de brancher votre système à un supresseur de surtension, et de débrancher toutes les lignes de télécommunications de votre modem durant un orage.
- Muni d'une prise murale correctement mise à la terre.

Ne pas utiliser ni modifier le câble d'alimentation C. A. fourni, s'il ne correspond pas exactement au type requis.

Assurez vous que le système soit débranché de son alimentation ainsi que de toutes les liaisons de télécomunication, des réseaux, et des lignes de modem avant d'enlever le capot. Ne pas utiliser le système quand le capot est enlevé.

WARNUNG

- Das System wurde für den Betrieb in einer normalen Büroumgebung entwickelt. Der entwickelt. Der Standort sollte:
- sauber und staubfrei sein (Hausstaub ausgenommen);
- gut gelüftet und keinen Heizquellen ausgesetzt sein (einschlie?lich direkter Sonneneinstrahlung);
- keinen Erschütterungen ausgesetzt sein;
- keine starken, von elektrischen Geräten erzeugten elektromagnetischen Felder aufweisen;
- in Regionen, in denen elektrische Stürme auftreten, mit einem Überspannungsschutzgerät verbunden sein; während eines elektrischen Sturms sollte keine Verbindung der Telekommunikationsleitungen mit dem Modem bestehen;
- mit einer geerdeten Wechselstromsteckdose ausgerüstet sein.

Versuchen Sie nicht, das mitgelieferte Netzkabel zu ändern oder zu verwenden, wenn es sich nicht um genau den erforderlichen Typ handelt.

Das System darf weder an eine Stromquelle angeschlossen sein noch eine Verbindung mit einer Telekommunikationseinrichtung, einem Netzwerk oder einer Modem-Leitung haben, wenn die Gehäuseabdeckung entfernt wird. Nehmen Sie das System nicht ohne die Abdeckung in Betrieb.

AVVERTENZA

Il sistema è progettato per funzionare in un ambiente di lavoro tipico. Scegliere una postazione che sia:

- Pulita e libera da particelle in sospensione (a parte la normale polvere presente nell'ambiente).
- Ben ventilata e lontana da fonti di calore, compresa la luce solare diretta.
- Al riparo da urti e lontana da fonti divibrazione.
- Isolata dai forti campi magnetici prodotti da dispositivi elettrici.
- In aree soggette a temporali, è consigliabile collegare il sistema ad un limitatore di corrente. In caso di temporali, scollegare le linee di comunicazione dal modem.
- Dotata di una presa a muro correttamente installata.

Non modificare o utilizzare il cavo di alimentazione in c. a. fornito dal produttore, se non corrisponde esattamente al tipo richiesto.

Prima di rimuovere il coperchio del telaio, assicurarsi che il sistema sia scollegato dall'alimentazione, da tutti i collegamenti di comunicazione, reti o linee di modem. Non avviare il sistema senza aver prima messo a posto il coperchio.

ADVERTENCIAS

El sistema está diseñado para funcionar en un entorno de trabajo normal. Escoja un lugar:

- Limpio y libre de partículas en suspensión (salvo el polvo normal)
- Bien ventilado y alejado de fuentes de calor, incluida la luz solar directa.
- Alejado de fuentes de vibración.
- Aislado de campos electromagnéticos fuertes producidos por dispositivos eléctricos.
- En regiones con frecuentes tormentas eléctricas, se recomienda conectar su sistema a un eliminador de sobrevoltage y desconectar el módem de las líneas de telecomunicación durante las tormentas.
- Previsto de una toma de tierra correctamente instalada.

No intente modificar ni usar el cable de alimentación de corriente alterna, si no se corresponde exactamente con el tipo requerido.

Asegúrese de que cada vez que se quite la cubierta del chasis, el sistema haya sido desconectado de la red de alimentación y de todos lo enlaces de telecomunicaciones, de red y de líneas de módem. No ponga en funcionamiento el sistema mientras la cubierta esté quitada.

Network Software License Agreement

BY USING THIS SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. DO NOT USE THIS SOFTWARE UNTIL YOU HAVE CAREFULLY READ AND AGREED TO THE FOLLOWING TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE SOFTWARE PACKAGE AND ANY ACCOMPANYING ITEMS.

License: Intel Corporation ("Intel") grants you the non-exclusive right to use the enclosed software program (the "Software"). You will not use, copy, modify, rent, sell or transfer the Software or any portion thereof except as provided in this Agreement.

You may:

1. Install/use the Software in a single computer or on a single local area network ("LAN") server;

2. Copy the Software solely for backup or archival purposes, including copying the Software into memory.

RESTRICTIONS

You **Will Not**:

1. Sublicense the Software;

2. Reverse engineer, decompile or disassemble the Software;

3. Copy the Software, in whole or in part, except as provided in this Agreement.

TRANSFER: You may transfer the Software to another party if the receiving party agrees to the terms of this Agreement and you retain no copies of the Software and accompanying documentation. Transfer of the Software terminates your right to use the Software.

OWNERSHIP AND COPYRIGHT OF SOFTWARE: Title to the Software and all copies thereof remain with Intel or its vendors. The Software is copyrighted and is protected by United States and international copyright laws. You will not remove the copyright notice from the Software. You agree to prevent any unauthorized copying of the Software.

DUAL MEDIA SOFTWARE: If the Software package contains multiple media, you may only use the disks appropriate for your single-user computer or LAN.

WARRANTY: The Software is provided "AS IS." Intel warrants that the media on which the Software is furnished will be free from defects in material and workmanship for a period of one (1) year from the date of purchase. Upon return of such defective media, Intel's entire liability and your exclusive remedy shall be the replacement of the Software.

THE ABOVE WARRANTY IS IN LIEU OF ANY OTHER WARRANTY, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OF ANY INTELLECTUAL PROPERTY, OR ANY WARRANTY ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

LIMITATION OF LIABILITY: NEITHER INTEL NOR ITS VENDORS SHALL BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF USE, LOSS OF DATA, INTERRUPTIONS OF BUSINESS, INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS, NOR FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND WHETHER UNDER THIS AGREEMENT OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

AUDIT: Intel reserves the right to have audits conducted to verify your compliance with this Agreement.

TERMINATION OF THIS LICENSE: Intel may terminate this license at any time if you are in breach of any of its terms and conditions. Upon termination, you will immediately destroy the Software or return all copies of the Software and documentation to Intel.

U.S. GOVERNMENT RESTRICTED RIGHTS: The Software and documentation were developed at private expense and are provided with "RESTRICTED RIGHTS". Use, duplication or disclosure by the Government is subject to restrictions as set forth in FAR 52.227-14 and DFAR 252.227-7013 et seq. or its successor.

EXPORT LAWS: You agree that the distribution and export/re-export of the Software is in compliance with the laws, regulations, orders or other restrictions of the U.S. Export Administration Regulations.

APPLICABLE LAW: Any claim arising under or relating to this Agreement shall be governed by the internal substantive laws of the State of Delaware or federal courts located in Delaware, without regard to principles of conflict of laws. Each party hereby agrees to jurisdiction and venue in the courts located in the State of Delaware for all disputes and litigation arising under or relating to this Agreement. This provision is meant to comply with 6 Del. C. Section 2708(a).

B Technical Specifications

General Specifications

Physical specifications

The physical specifications for the Express Router are as follows:

Dimensions (h × w × d)	2.4 × 9.5 × 9.8 inches (60 × 24 × 25 cm)
Weight (approximate)	2 lb. 10 oz. (1.2 kg)
Recommended clearance	1.5 inches (40 mm) sides, 4 inches (100 mm) rear

Power requirements

The power requirements for the Express Router are as follows:

Nominal power supply voltages	100 — 250 V AC (±10%) 50 — 60 Hz Class I
Current consumption	0.3A AC
Power consumption	14 W
Mains connection	External Power Supply Unit

Environmental

The environmental specifications and considerations for the Express Router are:

Temperature	Operating: +41 — 104°°F (+5 — +40°C) Storage: –13 — 158°°F (–2° — +70° C)
Humidity	5 — 95% non-condensing
Altitude	Up to 10000 feet (3480 m)

Approvals

The router complies with these approval requirements:

Safety	UL 1950 CSA-C22.2 No. 950 IEC 950 EN 60950
Telecommunications	CTR 1 CTR 2 FCC part 68 IC CS-03
Emission	47 CFR part 15 Class A EN 55022 Class A CISPR 22 Class A CNS 13438 Class A
Susceptibility	EN 55024 CISPR24 EN 50082-1
CE Mark	Yes

Hardware Specifications

CPU

The Express Router is equipped with the following RISC processors:

Product Code	Processor
ER8210, ER8220, ER930, ER9535	Intel i960®JT processor 100 MHz

DRAM and flash memory

The Express Router is equipped with the following:

Product Code	DRAM	Flash memory
ER8210, ER8220	16 MB	8 MB
ER9530, ER9535	32 MB	16 MB

LED indicators

The functions of the LED indicators on the front of the Express Router are described in “LED Descriptions”, p. 5.

LAN Ports

10/100 Mbps LAN ports

The 10/100Mbps LAN port supports a 10Base-T or 100Base-T connection for transmission speeds of up to 10 Mbps or 100Mbps respectively.

The LAN port is an RJ-45 socket to attach Unshielded Twisted Pair (UTP) as a medium for Local Area Networks (LANs) conforming to IEEE 802.3. Other Ethernet types must use an external adapter.

10 Mbps LAN ports

The 10 Mbps LAN port supports a 10Base-T connection for transmission speeds of up to 10 Mbps.

The LAN port is an RJ-45 socket to attach Unshielded Twisted Pair (UTP) as a medium for Local Area Networks (LANs) conforming to IEEE 802.3. Other Ethernet types must use an external adapter.

WAN Ports and Interface Cables

WAN ports

WAN ports on the Express Router terminate with a 50-pin SCSI type (female) connector to support the following interfaces by using the appropriate adapter cable:

Interface	Cable	Associated Standards
V.24	ER0001CB	V.24 defined by CCITT standard V.28, V.24 ISO 2110.
V.35	ER0002CB	V.35 defined by CCITT standard V.28, V.35, ISO 2593.
V.36	ER0003CB	V.36 defined by CCITT standard V.10, V.11, V.36, ISO 4902.
X.21/V.11	ER0004CB	X.21/V.11 defined by CCITT standard V.11, X.21, ISO 4903.

V.24 Interface and Cable

Connector type and pin designation

The ER0001CB V.24 WAN connect cable is terminated with a male 50-pin SCSI type connector on the router end and a male 25-pin D-sub connector (ISO2110) providing the V.24 interface. The pin designations are:

Router end	Signal	V.24	Direction[1]	CCITT Ref.
1	SHIELD	1	-	101
	GND (signal ground)	7	-	102
21	TxD (transmit data)	2	output	103
36	RxD (receive data)	3	input	104
18	RTS (request to send)	4	output	105
39	CTS (clear to send)	5	input	106
38	DSR (data set ready)	6	input	107
17	DTR (data terminal ready)	20	output	108
40	DCD (data carrier detect)	8	input	109

Router end	Signal	V.24	Direction[1]	CCITT Ref.
35	TxC (transmit clock)	15	input	114
37	RxC (receive clock)	17	input	115
14	CI (call indicator)	22	input	125
19	RL (remote loop)	21	output	140
20	LL (local loop)	18	output	141
15	TI (test indicator)	25	input	142
16	(shorted)	—	—	—
50		—	—	—
24	(shorted)	—	—	—
27		—	—	—
31		—	—	—
5	(shorted)	—	—	—
26		—	—	—
30		—	—	—

[1] Direction is given with respect to the router

CCITT classification

The V.24 WAN connector is classified as DTE according to the CCITT recommendation, and uses synchronous full-duplex communication.

Transmission speed of a V.24 connection

A WAN port configured as V.24 provides data transmission rates of up to 128 kbps.

Intended use

The V.24 interface is intended for use with a wide-band (high-speed) modem.

V.35 Interface and Cable

Connector type and pin designations

The ER0002CB V.35 WAN connect cable is terminated with a male 50-pin SCSI type connector on the router end and male 34-pin Winchester connector (ISO2593) providing the V.35 interface. The pin designations are:

Router end	Signal	V.35	Direction[1]	CCITT Ref.
1	SHIELD	A	-	101
	GND	B	-	102
49	TxDA	P	output	103
48	TxDB	S	output	
3	RxDA	R	input	104
2	RxDB	T	input	
18	RTS	C	output	105
39	CTS	D	input	106
38	DSR	E	input	107
17	DTR	H	output	108
40	DCD	F	input	109
11	TxCA	Y	input	114
10	TxCB	AA	input	
7	RxCA	V	input	115
6	RxCB	X	input	
14	CI	J	input	125
19	SHIELD	N	output	140
20	LL	L	output	141
15	TI	NN	input	142
16	(shorted)	—	—	—
50		—	—	—

Router end	Signal	V.35	Direction[1]	CCITT Ref.
26	(shorted)	—	—	—
50		—	—	—
24	(shorted)	—	—	—
27		—	—	—

[1] Direction is given with respect to the router

CCITT classification

The V.35 WAN port is classified as DTE according to the CCITT recommendation, and uses synchronous full-duplex communication.

Transmission speed of a V.35 connection

A WAN port configured as V.35 provides data transmission of up to 2 Mbps.

Intended use

A V.35 interface is intended for use with a wide-band (high-speed) modem.

V.36 Interface and Cable

Connector type and pin designations

The ER0003CB V.36 WAN connect cable terminates with male 50-pin SCSI type connector on the router end and a male 37-pin D-sub connector (ISO4902) to provide the V.36 interface. The pin designations are:

Router end	Signal	V.36	Direction[1]	CCITT Ref.
1	SHIELD	1	—	101
	GND	19	—	102
44	TxDA	4	output	103
43	TxDB	22	output	
3	RxDA	6	input	104
2	RxDB	24	input	104

Router end	Signal	V.36	Direction[1]	CCITT Ref.
46	RTSA	7	output	105
45	RTSB	25	output	
29	CTSA	9	input	106
28	CTSB	27	input	
27	DSRA	11	input	107
26	DSRB	29	input	
42	DTRA	12	output	108
41	DTRB	30	output	
31	DCDA	13	input	109
30	DCDB	31	input	
11	TxCA	5	input	114
10	TxCB	23	input	
7	RxCA	8	input	115
6	RxCB	26	input	
33	CI	15	input	125
47	RL	14	output	140
50	GND	37	—	102a
25	LL	10	output	141
32	TI	18	input	142
34	GND	20	—	102b
24	(shorted)	—	—	—
40		—	—	—

[1] Direction is given with respect to the router

CCITT classification

The V.36 WAN port is classified as DTE according to the CCITT recommendation, and uses synchronous full-duplex communication.

Transmission speed of a V.36 connection

A WAN port configured as V.36 provides data transmission of up to 2 Mbps.

Intended use

A V.36 interface is intended for use with a wide-band (high-speed) modem.

X.21/V.11 Interface and Cable

X.21/V.11 cable connectors and pin designations

The ER0004CB X.21/V.11 WAN connect cable is terminated with a male 50-pin SCSI type connector on the router end and a male 15-pin D-sub connector (ISO 4903) providing the X.21/V.11 interface. The pin designations are:

Router end	Signal		X.21/ V11	Direction[1]
1	SHIELD		1	-
44	TA	(transmit data: wire A)	2	output
46	CA	(control: wire A)	3	output
3	RA	(receive data: wire A)	4	input
31	IA	(indication: wire A)	5	input
7	SA	(signal element timing: wire A)	6	input
1	GND	(signal ground)	8	-
43	TB	(transmit data: wire B)	9	output
45	CB	(control: wire B)	10	output
2	RB	(receive data: wire B)	11	input
30	IB	(indication: wire B)	12	input
6	SB	(signal element timing: wire B)	13	input
24	(shorted)		—	—
39			—	—

[1] Direction is given with respect to the router

CCITT classification

The X.21/V.11 WAN connector is classified as DTE according to the CCITT recommendation, and uses synchronous full-duplex communication.

Transmission speed of X.21/V.11 connection

The X.21/V.11 WAN port can only be used for leased line connections, which provide data transmission rates of up to 2 Mbps.

Intended use

An X.21/V.11 interface is intended for use with a wide-band (high-speed) modem.

CSU/DSU Ports and Cables

CSU/DSU port

A CSU/DSU port on an Express Router supports direct connection to a T1 interface providing transmissions speeds of up to 1.544 Mbps. The CSU/DSU port terminates with a 15-pin D-sub male connector.

CSU/DSU Cables and pin designations

The Express Router that has CSU/DSU port is supplied with a DB15-to-RJ48C cable and a DB15-to-RJ48C adapter for connection to a T1 line. A DB15-to-DB15 T1 interface cable (product code ER0005CB) is also available for purchase. CSU/DSU cables are green in color.

DB15 to RJ48C Cable

The router end of the cable is terminated with a 15-pin D-sub female connector. The T1 end of the cable is terminated with an RJ48C connector. The pin designations are as follows.

Router end (DB15)	Signal	T1 (RJ48C)	Direction[1]
3	R1	1	Input
11	T1	2	Input
1	R	4	Output
9	T	5	Output

DB15 to RJ48C Adapter

The router end of the adapter is terminated with a 15-pin D-sub female connector.The T1 end of the adapter has an RJ48C socket. The pin designations are as follows.

Router end (DB15)	Signal	T1 (RJ48C)	Direction[1]
3	R1	1	Input
11	T1	2	Input
1	R	4	Output
9	T	5	Output

DB15 to DB15 T1 Cable (ER0005CB)

The router end of the cable is terminated with a 15-pin D-sub female connector. The T1 end of the cable is terminated with a 15-pin D-sub male connector. The pin designations are as follows.

Router end	Signal	T1 (DB15)	Direction[1]
3	R1	3	Input
11	T1	11	Input
1	R	1	Output
9	T	9	Output
2	GND	2	—
4	GND	4	—

[1] Direction is given with respect to the router

Console Port and Supported Modems

Console Port

The console port on the router is a DB9 male connector for asynchronous serial RS-232 communication. The console port can be configured for communication with a VT100-compatible terminal or for PPP via an asynchronous modem.

Terminal communication parameters

When configured for terminal communication, the console port operates on the following parameters:

- baud rate 9.6 kbps
- 8-bit data
- no parity
- 1 start bit
- 1 stop bit

Console port terminal cable and pin designations

The terminal cable suppled with the router is terminated with a DB9 female connector on each end. The pin assignments are;

DB9 female	Signal	DB9 female	Direction[1]
1	DCD (data carrier detect)	4	input
6	DSR (data set ready)		
2	RX (receive data)	3	input
3	TX (transmit data)	2	output
4	DTR (data terminal ready)	1	output
		6	output
5	GND (signal ground)	5	—
7	RTS (request to send)	8	output
8	CTS (clear to send)	7	input
Shield	CRI	—	—

[1] Direction is given with respect to the router

Supported Modems

Supported Modems

The asynchronous modems supported for PPP dial-up connections via the console port are listed below, along with the initialization strings required for their proper operation.

3Com (USRobotics) Courier V.Everything§ Corporate Modem

init. string 1	ATZ
init string 2	AT&F0X4E0V1S0=0&D2&I0&K0&R2&B1
init. string 2 (slow)	AT&F0X4E0V1S0=0&D2&I0&K0&R2&B1&N8 &H1
AT command description	&F0 - Factory default template X4 - Result code set X4 E0 - Command mode echo off V1 - Return code in verbal mode S0=0 - Disable auto answer &D2 - Normal DTR operations &C0 - Carrier Detect operations. CD always on. &I0 - Disables XON/XOFF flow control &K0 - Data compression disabled &R2 - Hardware flow control enabled &B1 - Fixed serial speed (router UART speed) &N8 - Sets speed to 14.4 Kbps &H1 - Hardware flow control

3Com (USRobotics) Sportster Flash§

init. string 1	ATZ3
init. string 2	AT&F0X4E0V1S0=0&D2&I0&K0&R2&B1L0&H1
init. string 2 (slow)	AT&FX4E0V1S0=0&D2&I0&K0&R2&B1L0&H1&N8&H1
AT command description	&F - Factory default template X4 - Result code set X4 E0 - Command mode echo off V1 - Return code in verbal mode S0=0 - Disable auto answer &D2 - Normal DTR operations &I0 - Disables XON/XOFF flow control &K0 - Data compression disabled &R2 - Hardware flow control enabled &B1 - Fixed serial speed (router UART speed) L0 - Low speaker volume &N8 - Sets speed to 14.4 Kbps &H1 - Hardware flow control

GVC 56k Speakerphone§ (SF-1156V/R21)(

init. string 1	ATZ0
init. string 2	ATX4E0V1S0=0&D2&K3%C0
init. string 2 (slow)	ATX4E0V1S0=0&D2&K3%C0+MS=10,1,300,144
AT command description	&F0 - Factory default template settings X4 - Response, dial tone, busy signal detection E0 - Echo off V1 - Word responses S0=0 - Disable auto answer &D2 - Modem hags up, returns to Command mode after DTR toggle &K3 - Enables RTS/CTS hardware flow control %C0 - Disable MNP Class 5 and V.42bis data compression +MS=10,1,300,144 - Sets speed to 14.4 Kbps

The listed models have been tested for use with the Express Router. Other modems can be used, however their compatibility cannot be guaranteed. Refer to your modem documentation for details.

Note The AT commands must be configured in order for the modem to operate properly. If you are configuring a non-supported modem, it is recommended that you use the modems above as examples.

Supported Connections

Number of connections supported

Use this table to determine the number of connections supported in the router based on connection types used.

Router	Maximum connections per type					Maximum connections in router
	PPP leased line	Frame Relay	X.25	PPP modem	Tunnel	
8210	1	60	60	60	10	60
8220	1	60	60	60	10	60
9530	2	59	59	59	10	59
9535	2	59	59	59	10	59

Connections can be added until the limit is reached for either the connection type or the maximum number of connections in the router.

Example:

An Express 8210 Router with 10 tunnel connections can have up to 50 Frame Relay connections: 60 -10 = 50.

Network and Bridging Protocols

RFCs

The following RFCs are supported by the Express Router:

RFC	Description
768	User Datagram Protocol (UDP)
783	Trivial File Transfer Protocol (TFTP) revision 2
791	Internet Protocol (IP)
792	Internet Control Message Protocol (ICMP)
793	Transmission Control Protocol (TCP)
826	Ethernet Address Resolution Protocol (ARP)
877	Transmission of IP Datagrams Over Public Data Networks
919	Broadcasting Internet Datagrams
922	Broadcasting Internet Datagrams in the Presence of Subnets
950	Internet Standard Subnetting Procedure
951	Bootstrap Protocol
1027	Using ARP to Implement Transparent Subnet Gateways
1058	Routing Information Protocol (RIP)
1075	Distance Vector Multicast Routing Protocol (DCMRP)
1112	Internet Gateway Multicast Protocol (IGMP)
1155	Simple Network Management Protocol (SNMP)
1166	Internet Numbers
1212	Concise MIB Definitions
1213	Management Information Base for Network Management of TCP/IP-Based Internets: MIB II
1256	Internet Control Message Protocol (ICMP) Router Discovery Messages

RFC	Description
1315	Management Information Base (MIB) for Frame Relay Data Terminal Equipment (DTE), 1992
1356	Multiprotocol Interconnect on X.25
1490	Multiprotocol Interconnect over Frame Relay Data Terminal Equipment (DTE), 1993
1493	Definition of Managed Objects for Bridges
1631	Network Address Translation (NAT)
1700	Assigned Numbers
1723	Routing Information Protocol (RIP) Version 2
1812	Requirements for IP Version 4 Routers — regarding subnetting
2091	Triggered RIP
2205	ReSerVation Protocol (RSVP)
2206	Management Information Base (MIB) for ReSerVation Protocol (RSVP)
2236	Internet Group Management Protocol, version 2.0

IP Multicast routing

The Express Router supports IP Multicast routing using MROUT-D version 3.8 which consists of the following protocols:

- Distance Vector Multicast Routing Protocol (DVMRP) version 3
- Internet Group Multicast Protocol (IGMP) version 2

Novell specifications

IPX Router Specification, Novell part No. 107-000029-001.

Novell NetWare Link Services Protocol Specification Rev 1.0, Novell part No. 100-001708-002.

Bridging

IEEE/ANSI Standard 802.1D, and IEEE/ANSI 820.1G: Spanning Tree Bridging

ISO 10038: MAC Bridges.

WAN Protocols

Leased line

The Express Router supports leased line connections using the PPP protocol. Leased line connection services are available for all the connections supported off WAN ports and CSU/DSU ports.

PPP standards

PPP in the Express Router support these RFCs:

RFC	Description
1332	Internet Protocol Control Protocol (IPCP) for the Point-to-Point Protocol (PPP)
1334	Password Authentication Protocol (PAP)
1552	Internetwork Packet Exchange§ Protocol Control Protocol (IPXCP) for the Point-to-Point Protocol (PPP)
1638	Bridge Control Protocol (BCP) for the Point-to-Point Protocol (PPP)
1661	Link Control Protocol (LCP) for the Point-to-Point Protocol (PPP)
1662	Point-to-Point Protocol (PPP) over High-level Data Link Control (HDLC)
1962	Point-to-Point Protocol (PPP) Data Compression
1968	Point-to-Point Protocol (PPP) Encryption
1974	Point-to-Point Protocol (PPP) Stac Data Compression
1994	Challenge Handshake Authentication Protocol (CHAP)

HDLC

The Express Router supports leased line connections and dial-up connections over HDLC, conforming to the following:

High-level Data Link Control
ISO/IEC 3309

Frame Relay protocol

The Express Router supports the Frame Relay protocol, conforming to the following:

Standard	Description
FRF.1	Frame Relay User-Network Interface, January 1992
FRF.3	Frame Relay Multiprotocol Interconnect, December 1992
ANSI T1.606	Frame Relaying Bearer Service Architectural Framework and Service Description 1990
	Frame Relaying Bearer Service, Congestion Management Principles, 1991 Addendum 1
ANSI T1.617	DSS1 — Signalling Specification for Frame Relay Bearer Service, 1991
ANSI T1.618	DSS1 — Core Aspects of Frame Protocol for use with Frame Relay Bearer Service, 1991
ITU-T (CCITT) I.233.1	Frame Relay Bearer Services, 1991
ITU-T (CCITT) I.370	Congestion Management in Frame Relaying Networks, 1991
ITU-T (CCITT) Q.922	ISDN Data Link Layer Specification for Frame Mode Bearer Services, 1992

X.25 protocol

The Express Router supports the X.25 protocol, conforming to the following standards:

Standard	Description
ITU-T (CCITT) X.121	International Numbering Plan for Public Data Networks
ITU-T (CCITT) X.25	Interface Between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DTE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuits
ISO/IEC 7776	Link Access Procedure, Balanced (LAPB)
ISO/IEC 8208	X.25 Packet Layer Protocol for Data Terminal Equipment (DTE)

IPX WAN services

The IPX WAN2 Protocol is supported via both Numbered and Unnumbered WAN connections.

Boot Sources

Flash memory

Under normal circumstances, the router will always boot from the internal flash memory. No external boot source is required.

BootP/TFTP

Boot via LAN and WAN using the BootP/TFTP protocol can only be used as a backup against flash memory failure.

SNMP Management

SNMP

An SNMP agent according to RFC 1213 (MIB-II).

I Index

Numerics

10 Mbps LAN port
  connecting, 27
  description, 4
  specifications, 319
10/100 Mbps LAN port
  connecting, 26
  description, 4
  specifications, 319
100Base-T, 319
10Base-T, 319

A

Abbreviations list, xx
Access for
  gas pump configuration, 260
Access restrictions
  bridging forwarding tables, 229
  call direction, 147
  controlled bridging, 233
  Daily Activity Limit, 149
  for the router, 248
  IP filters, 167
  IPX data filters, 215
  IPX RIP and SAP filters, 210
  Timer Profiles, 150
Accounting, link, 149
Acrobat Reader, installing, 34
Acronyms list, xx
Activity on the LAN and WAN links, 76
Address
  IPX network, Advanced Setup, 208
Advanced
  link facilities and parameters, 146
Advanced Setup
  access from Intel Device View, 92
  access from Local Management, 92
  access via a Telnet session, 92
  finishing, 96
  general description, 91
  general use, 91
  on-line help, 96
  overview, 94
  to exit, 97
AMI line coding, 100, 101
Approvals, 318
Atmospheric pressure specifications, 318
Authentication
  RIP-2, 160
Authentications, 72
Auto Fix, Intel Device View Diagnostics, 49,

283

B

B8ZS line coding, 100, 101
Backup
connection scenario, Connection Setup, 59
for another link or port, 147
Backward Explicit Congestion Notification, see also BECN, 110
Bandwidth weight
Frame Relay link, 110, 117
Bc
Frame Relay link, 116
BCIQ (Taiwan) declarations, xvii
Be
Frame Relay link, 116
BECN
configure for Frame Relay link, 117
description, 110
Boot process, 302
Boot sources, 336
BootP Request Forwarding, IP routing, 160
Branch systems (UK only), xvi
Bridging
adding to a link, 227
Advanced screen, 228
configuration, 225
controlled, 233
duplicate frames seen, troubleshooting, 297
enabling/disabling, 227
Forwarding Table examples, 231
implementation, 225
long delays occurring, troubleshooting, 298
monitoring, 77
Multicast Forwarding Table, 229
restricting multicasts, 235
Source Forwarding Table, 230
Spanning Tree parameters, 228
specifications, 332, 333
spoofing, 226
support, 20
troubleshooting, 297
Type (packet type) Forwarding Table, 230
unable to forward IP data, troubleshooting, 298
unable to forward IPX data, troubleshooting, 297
Unicast Forwarding Table, 229

C

Cables for WAN port, 24
Call
direction parameters, 147
Retry Limit exceeded, 49
setup parameters, 148
timing setup, 148
Call-back
PPP dial-up modem link, 127
X.25, see X.25 Reverse Charges
Caution
EMC, xi
CD ROM, 24
CE Mark, approval, xvii, 318
Channel allocation (CSU/DSU), 100
Channel bandwidth
CSU/DSU parameter, 101
Channel speed (CSU/DSU, T1), 100
CIR
Frame Relay link, 116
Clock, router, 72
Command line configuration, 264
command prompt, 265
commands, 265
description, 10
exit, 266
syntax, 265
Committed Burst, see also Bc, 116
Committed Information Rate (CIR), 116
Community
SNMP router access, 249
Components check list, 23
Config.p file, gas pump configuration, 261
Config.txt file
example files, 276
gas pump configuration, 261

Configuration, 70
Advanced Setup, 91
BPDUs, bridging, 226
command line configuration, 264
dynamic, 96
exit, 97
gas pump configuration, 260
options for the router, 99
resetting to factory default, 307
restore backup, 71
restore to factory default, 72
router starting with old, troubleshooting, 287
save new, 97
save to flash memory, 70
saving permanently, 70
Configuration management, 70
Configuring
a leased line, 103
an Internet Tunnel, 131
bridging services, 225
CHAP on a PPP link, 144
Frame Relay services and links, 109
IP filtering on a link, 174
IP Multicast Tunnels, 162
IP routing, 153
IP RSVP, 164
IP static routes, 200
IPX data filtering on a link, 216
IPX RIP and SAP filtering on a link, 211
IPX static routes and services, 220
management of the router, 248
Novell IPX routing, 203
timer profiles on a link, 150
X.25 services and links, 118
Conf-res.txt file, gas pump configuration, 261
Connection Setup, 58
accessing, 59
adding connections, 61
backup connection scenario, 59
configuring the console port, 60
configuring WAN ports, 60
direct connection to remote site scenario, 58
Internet access scenario, 58
scenarios, 58
Wizards, using Advanced Setup after, 91
Connections, number supported, 331
Console cable
specifications, 328
Console mode, 252
Console port
access to Local Management, 84
configuring for dial-up modem, 124
configuring from Intel Device View, 61
connecting a terminal or PC, 30
connecting dial-up modem, 29
description, 4
Local Management via dial-in modem connection, 86
port specifications, 327
setting to console mode, 61, 252
setting to modem mode, 127, 252
terminal cable, 24
terminal parameters, 31
troubleshooting, 288
Contact person
assigning, 96
for router, 72
Controlled bridging, 233
CPU type, 318
CSU/DSU, 99
channel allocation, 100
channel bandwidth, 101
channel speed, 100
configuring, 101
data inversion, 101
fractional T1, 11, 99
framing format parameter, 100, 101
full T1, 99
line build out, 102
line code parameter, 101
line coding, 100
line speed, 100
T1 support, 11
timing mode, 102
troubleshooting, 290
CSU/DSU cables, 24
specifications, 326
CSU/DSU port
configuring using Intel Device View, 60
connecting, 29
description, 4
LEDs, 7

port specifications, 326
Current consumption, 317
Custom Modem Profile, 128

D

D4, 100, 101
Daily Activity Limit
exceeded, 49
WAN link facility, 149
Data compression
Frame Relay, 11
Frame Relay link, 117
Internet Tunnel, 134
parameter, 105, 108
PPP, 15
PPP dial-up modem link, 126
X.25, 13
X.25 link, 13, 121
Data inversion parameter, CSU/DSU, 101
Data Link layer service, see Bridging
Date and time in the router, 72
Default Action
IP filters, 174
Novell IPX RIP filters, 212
Novell SAP filters, 211
Default Packet Size
X.25 port, 120
Default setup
Frame Relay, 12, 111
Destinations for SNMP traps, 72
Details in Intel Device View, 77
Device and Hardware information, 76
Device Discovery, 43
See also Device Tree
setting options, 44
Device Setup
options for the router, 99
router starting with old configuration, troubleshooting, 287
saving, 97
Device Tree, 43
adding a device, 45
deleting a device, 45
device discovery options, 44
icons, 44
DHCP Forwarding, IP routing, 160
DHCP Server
configuring DNS server, 64
configuring from Advanced Setup, 242
configuring from Intel Device View, 63
editing IP address ranges, 64
enabling, 64
IP addresses, 242
lease time, 242
overview, 20, 241
Diagnostics
autofix, 49
message level, 48
Dial-up modem
installation, 29
supported, 29
Dial-up modem connections
see PPP dial-up modem link, 123
support, 14
Direct connection to remote site, Connection Setup scenario, 58
Disable connection, Intel Device View, 57
Discard filter, Log system, 256
Distribution of link traffic, Intel Device View Explorer, 56
DLCI
Frame Relay, 113, 115
DLCMI
Frame Relay, 112, 114
DMZ, 170
DNS server
configure router for use with, 202
configuring with DHCP server, 64, 243
Domain Name System (DNS) server, see DNS server
DRAM, 319
DTE port cables, 24
DVMRP
Metric, IP Multicast routing, 160
Metric, IP Multicast Tunnel, 164
Dynamic
configuration, 96
IP Address, 159
IP address assignment, 18
IP routing (RIP), 153
IPX routing (RIP and SAP), 203
Mapping, NAT, 194

Dynamic Host Protocol Configuration Protocol Server, see DHCP server

E

Earthing (grounding)
requirements, 27, 30
EEC declarations, xiv
EMC caution, xi
Emission approvals, xvii, 318
Enable connection, Intel Device View, 57
Enabling
bridging services, 227
IP routing, 156
IPX routing, 207
Encapsulation Type, X.25, 122
Equipotential bonding requirements, 27, 30
ESF, 100, 101
Example
bridge forwarding tables, 231
Internet Tunnel and basic Internet access filters, 139
Internet Tunnel with Internet access, 135
Network Address Translations (NAT), 198
Novell IPX data filtering, 219
static backup route, Novell IPX, 223
Excess Burst, see also Be, 116
Explorer, 54

F

Factory default configuration, resetting to
from Intel Device View, 72
using the recovery button, 307
Factory default setup, 21
FCC statements, xii
Filtering parameter
IP Multicast Tunnel, 163
IP routing, 158
Filters
bridge forwarding tables, 229
IP, see IP filters
IPX data, see Novell IPX filters, 215
IPX, see Novell IPX filters
Novell IPX RIP and SAP, 210
Firewall
description, 17
DMZ, 170
filter criteria, 176
filters, see also IP filters
Intel Device View, 68
port to application mapping, 17, 171, 178
receive filters, 169
stateful filter, 17
stateful filter example, 183
stateful filters, 167, 175
static filter, 17
static filter example, 180
SYN flood protection, 17, 172, 173
transmit filters, 169
Firmware
restore backup, 74
upgrade, 73
upgrade detection, 60
Flash memory, 319
load configuration from, 70
saving a new configuration to, 70
FlashPROM, 302
Flow control
description, 12
frame relay, 110
X.25 Port, 119
Forcing connection
down, Intel Device View, 57
up, Intel Device View, 56
Forwarding tables (bridging)
examples, 231
Multicast destination, 229
source-destination, 230
Type (packet type), 230
Unicast destination, 229
Fractional T1, 99
Frame Relay
configuration overview, 111
configure a link, 114
data compression, 11
default setup, 12, 111
description, 11, 109
DLCI, 113, 115
DLCMI, 112, 114

flow control
description, 12
services and links configuration, 109
specifications, 335
Framing format
CSU/DSU, 100, 101
Full T1, 99

G

Gas pump configuration, 260
access, 260
commands, 265
description, 10
errors file, 261
example Config.txt files, 276
exit, 266
file syntax, 265
files used, 261
General problems, see troubleshooting
Grounding (earth)
requirements, 27, 30

H

Hardware
information, 76
specifications, 318
Hello packets, bridging, 226
Highest 2-way Channel, X.25 port, 119
Humidity specifications, 318

I

icons, device tree, 44
IGMP, see IP Multicast routing
Industry Canada notice, xiii
Installation
of Intel Device View, 32
procedure, 25
warnings, 23
Intel Device View
as Plug-in, 9
CD ROM, 24
configuring ports, 60
Connection Setup, 57
accessing, 59
adding connections, 61
configuring connections, 61
configuring WAN ports, 60
scenarios, 58
description, 37
details, 77
device and hardware information, 76
Diagnostics
Auto Fix, 49, 283
corrective action, 49, 283
locate problem, 283
disabling/enabling connection, 57
Discovery
using, 45
Explorer, 54
distribution, 56
link not operational, 284
organization of information, 54
use of in troubleshooting, 284
Firmware Upgrade, 73
Install Wizard, 38
installation, 32
LAN and WAN link
activity, 76
overview, 77
LEDs, 42
load configuration from flash memory, 70
management of the router, 37
Monitor preferences, 79
monitoring
routing protocols and bridging, 77
the router, 76
On-line help, 40
opening router for management, 39
plotting, 78
polling parameters, 79
requirements, 32
resetting to factory default configuration, 72
restore backup configuration, 71

router firmware management, 73
router management setup, 72, 247
Router Setup access, 57
save configuration
permanently, 70
to flash memory, 70
starting
for Web, 38
for Windows, 38
System Window, 51
Trap Window, 50
troubleshooting with, 284
troubleshooting with, 281
Web
client requirements, 33
description, 8
server requirements, 32
Windows
description, 8
main display, 41
requirements, 32
Internet Access, Connection Setup scenario, 58
Internet routing, see Internet Tunnel
Internet Tunnel
and Internet access considerations, 132
configuration overview, 132
configuring, 131
data compression, 134
example, 135
IP static host router to the remote router, 131, 134, 201
Local IP Address, 134
Remote IP Address, 134
security over X.25 links application, 143
support, 16
use of NAT for security, 132
IP
Network Address Translation (NAT), 19
IP address
DHCP Server, 242
setting in Advanced Setup, 156
setting in Intel Device View, 38, 62
IP filters, 167
configuring, 174
configuring, Intel Device View, 68
criteria, 176
default action, 175
direction, 169
DMZ, 170
enabling, 158
example, 180
Logging, 175
logging, 170
packet processing, 169
port to application mapping, 171, 178
receive, 169
stateful, 167
stateful filter example, 183
stateful filters, 175
stateful pass filters, 167
static, 167
static filter example, 180
SYN flood protection, 172
transmit, 169
IP Multicast routing
Distance Vector Multicast Routing Protocol (DVMRP), 155
DVMRP metric, 160
enabling, 158
Internetworking Group Multicast Protocol (IGMP), 155
introduction, 18
protocol standards, 333
TTL Threshold, 161
IP Multicast Tunnels
Advanced screen, 163
configuring, 162
description, 162
DVMRP metric, 164
Filtering parameter, 163
introduction, 18
TTL Threshold, 164
IP Resource Reservation Protocol (RSVP)
configuring, 164
IP routing
adding to a link, 157
Advanced screen, 159
Authentication, RIP-2, 160
BootP / DHCP Forwarding, 160
configuration, 153
configuring static routes, 200
DVMRP metric, 160

dynamic, 153
IP Address, 159
IP address assignment, 18
enabling/disabling, 156
Filtering parameter, 158
filters, 19
example for Internet Tunnel, 139
Local IP Address, Internet Tunnels, 134
monitoring, 77
Multicast Tunneling, see IP Multicast Tunneling
Multicasts, see IP Multicast
multimedia protocols, 18
NAT, see Network Address Translation (NAT)
numbered links, 158
Protocol parameter, 158
ProxyARP, 160
Remote IP Address, Internet Tunnels, 134
RFCs, 332
RIP, 153
metric, 160
RIP-1 and RIP-2 support, 17
RSVP, support, 18
static, 154
host route for Internet Tunnels, 131, 134, 201
routes, 20
routes, configuring with Intel Device View, 67
support, 17
Triggered RIP
over dial-up links, 158
parameter, 158
support, 18
troubleshooting, 293
TTL Threshold, 161
unable to bridge IP data, troubleshooting, 298
will not forward data, troubleshooting, 293
IP, see IP routing
IPX data filters
defined on a link basis, 215
packet processing, 215
IPX, see Novell IPX routing
Isolating problems, see troubleshooting

K

Keep-alive (Novell SPX)
packet spoofing, 206
packets, 205

L

LAN 1 port
connecting, 26
description, 4
LEDs, 5
LAN 2 port
connecting, 27
DMZ, 170
LEDs, 5
LAN link
adding bridging to, 227
adding IP routing to, 157
adding IPX routing to, 208
configuring Bridging services, 225
configuring IP filtering, 174
configuring IP routing, 153
configuring IPX data filtering, 216
configuring IPX RIP and SAP filtering, 211
configuring IPX routing on, 203
configuring with Intel Device View, 62
LAN port
configuring with Intel Device View, 62
connecting to, 26
description, 4
LEDs, 5
specifications, 319
Late-Breaking News, 24
Lease time, DHCP Server, 242
Leased line, see PPP leased line
LEDs
10 Mbps, 5
100 Mbps, 5
CSU/DSU, 7

flashing in sequence, 8
functions, 319
Intel Device View, 42
LAN, 5
Status, 5
use of for troubleshooting, 281
WAN, 6
Licensed software, 75
advanced setup, 75, 257
Intel Device View, 75
Limit transfer rate parameter
Frame Relay link, 117
Line build out, CSU/DSU, 102
Line code parameter, CSU/DSU, 101
line coding, CSU/DSU, 100
Line interface connections (UK only), xvi
Line speed, (CSU/DSU or T1), 100
Link
accounting, 149
activity, 76
limiting daily activity, 149
overview, 77
traffic distribution, 56
Links
maximum, 331
number supported, 331
Load configuration from flash memory, 70
Local, 282
Address
X.25 link, 121
IP Address, Internet Tunnels, 134
Local Management, 81
access
from Intel Device View, 82
restrictions, 88
using Telnet, 82
via console port, 84
defining access passwords, 73, 250
from dial-in modem connection on console port, 86
introduction to, 9, 81
Telnet on default IP address, 83
Location, system parameters, 72, 96
Log System
configuring, 253
discard filter, 256
message filtering, 254, 255
message levels, 254
send to SysLog, 256
Log, see Intel Device View Report Manager
Logging IP filters, 175
Logical Channel Number
X.25 link, 121
Lowest 2-way Channel
X.25 port, 119

M

MAC address, 25
LAN 2 (10 Mbps), 26
location, 25
Main lead wiring colour code, xii
Main power cable, 23
Main power supply
connection, 317
warning, xi, 25
Maintenance Mode, 301
Management
access via WAN links, 161
configuration, Advanced Setup, 247
configuration, Intel Device View, 72
Intel Device View, 37
of configurations in the router, 70
of the router firmware, 73
setup, 70
tools available, 336
Maximum transfer rate
Frame Relay link, 111, 116
Memory
DRAM, 319
flash, 319
Modem mode, 252
Modem Profile, 128
copying, 129
creating, 130
custom, 128
definition, 128
editing, 130
predefined, 128
selecting for ppp dial-up modem link, 125
Monitoring
the router, 76

Mulitlink, see PPP Multilink
Multicast
Destination Forwarding Table, bridging, 229
IP, see IP Multicast routing, 18
restricting, bridging, 235

N

Name, of router, 72, 94, 96
Network
protocol specifications, 332
services, 17
Network Address Translation (NAT), 192
configuration, Intel Device View, 65
Dynamic Mapping, 194
examples of use, 198
internal and external networks, 192
Single IP Address Mapping, 195
Static Mapping, 193
support, 19
table, 192
Nominal power supply voltages, 317
Notices & Warnings, xi
Novell IPX filters
data filters, 215
configuration, 216
criteria, 217
example, 219
data, enabling, 209
RIP and SAP, 211
filters, 210
RIP filter criteria, 214
SAP filter criteria, 213
Novell IPX routing
adding to a link, 208
Advanced screen, 208
configuration, 203
configuring static routes and services, 220
dynamic, 203
enabling/disabling, 207
example use of a static backup route, 223
filters, 19
IPX network address, Advanced Setup, 208
monitoring, 77
numbered links, 208
SPX keep-alive packets, 205
static, 203
static routes and services, 20
support, 20
troubleshooting, 295
Type 20 Broadcasts, 209
unable to bridge IPX data, troubleshooting, 297
WAN link will not forward data, 295
WAN protocol, 204
WAN services, 336
watchdog spoofing, 205
will not forward data, troubleshooting, 296
Novell SPX, see Novell IPX routing, 205
Numbered links
IP routing, 158
Novell IPX routing, 208

O

On-line help
Advanced Setup, 96
Intel Device View, 40
On-line Reference manual, 34, 40
OSPF, 18
Overview of
Advanced Setup of the router, 94
Frame Relay configuration, 111
Internet Tunnel configuration, 124, 132
leased line configuration, 104, 107
PPP dial-up modem links, 124
the LAN and WAN links, 77
X.25 configuration, 119
Own Username, CHAP and PAP, 145

P

panel
router back, 1
router front, 1

Password
CHAP and PAP, 145
local management, 73
TFTP, 73
Password Authentication Protocol, see PPP PAP
PDF
on-line reference manual, 34
Permanent Virtual Circuits (PVCs)
X.25, 118
Packet Size, 121
Window Size, 121
Phone number
PPP dial-up modem link, 126
Plotting counters and details, 78
Polling
community, 79
monitor, 79
setting intervals, 79
timeout, 79
Port Speed, PPP dial-up modem link, 125
Port to application mapping, 171, 178
description, 17
Power
consumption, 317
supply connecting, 31
supply voltages, 317
PPP
Authentication Required, CHAP and PAP, 145
CHAP and PAP configuration, 144
dynamic IP addressing, 18
leased line
configuration, 103
configuration overview, 104
specifications, 334
leased line configuration overview, 107
Own Username, CHAP and PAP, 145
Password, CHAP and PAP, 145
Reply to, CHAP and PAP, 145
standards, 334
Tunnels, 16
PPP dial-up modem link
Call-back, 127
configuration overview, 124
configuring
console port for modem, 124
links, 125
data compression, 126
multiple logical links, 124
phone number, 126
port speed, 125
selecting modem profile, 125
setting the console port to modem mode, 127
support, 14, 123
troubleshooting, 288
PPP leased line
configuration overview, 104, 107
description, 103
multilink, 106
to configure, 104
PPP Multilink
configuring, 107
description, 14, 106
Predefined Modem Profile, 128
Preferences for Intel Device View, 79
Problems which could be encountered
general, 287
see Troubleshooting
WAN links, 290
Procedure for
troubleshooting the router, 282
Procedure for configuring
a leased line, 103
an Internet Tunnel, 131
Bridging services, 225
CHAP and PAP on a link, 144
Frame Relay services and links, 109
IP
filtering on a link, 174
Multicast Tunnels, 162
routing, 153
RSVP, 164
static routes, 200
IPX
data filtering on a link, 216
RIP and SAP filtering on a link, 211
static routes and services, 220
management of the router, 248
Novell IPX routing, 203
PPP dial-up modem links on console port, 123

the CSU/DSU, 99
timer profiles on a link, 150
X.25 services and links, 118
Products
covered in this manual, xi
standard parts supplied, 23
ProxyARP, IP routing, 160
PVC
Packet Size
X.25 link, 121
parameters
X.25 link, 121

Q

Quick Start guide, 24

R

Reboot, 72
Recovery button
description, 4
to reset to a factory default configuration, 307
Recovery Mode, 301
boot process, 302
from Intel Device View, 303
from the console port, 305
use, 301
Reference Manual, on-line, 40
Remote
Address
X.25 link, 121
IP address, Internet Tunnel, 134
Reply to, CHAP and PAP, 145
Requirements for
Intel Device View for Windows, 32
Reset to factory default configuration
from Intel Device View, 72
using the Recovery button, 307
Resource Reservation Protocol (RSVP), see IP Resource Reservation Protocol (RSVP), 18
Restore
backup configuration, 71
configuration, 97
factory default, 72
Reverse Charging
X.25 link, 13, 122
RIP
Metric, IP routing, 160
RIP (Novell IPX)
filters, 210
Rx filters, 210
Tx filters, 210
RIP-1, 17
routing, 153
triggered, 154
RIP-2, 17
authentication, 160
routing, 154
triggered, 154
Router
time and date, 72
Router configuration
installation using Install Wizard, 38
using Advanced Setup, 91
using Intel Device View, 57
Routing
Protocol, IP routing, 158
services, 17
RPOA
X.25 link, 122
RSVP, see IP Resource Reservation Protocol (RSVP), 18

S

Safety
approvals, xvii, 318
statement, xv
SAP (Novell IPX)
filters, 210
Rx filters, 210
Tx filters, 210
Saving
a new router setup, 97
configuration to flash memory, 70

Scenarios, for Connection Setup, 58
Setting up the router, see Connection Setup
Setup
  advanced, 91
  command line configuration, 264
  default, 21
  gas pump configuration, 260
  introduction to, 91, 241
  saving permanently to flash memory, 70
Shielded cables, xi
Shiva Configurator
  installing, 35
Single IP Address Translation, NAT, 195
SNMP
  access rights, 248
  Advanced Setup management configuration, 247
  Community, router access, 249
  enabling access via WAN links, 161
  specifications, 336
  trap destinations, 72, 253
  trap, enabling, 249
Software
  Acrobat Reader, 34
  installation, 32
  Intel Device View, 32
  location, 302
  Shiva Configurator, 35
Software licensing, 75
  Advanced setup, 75, 257
  Intel Device View, 75
  licensed software, 267
Source Forwarding Table, bridging, 230
Spanning Tree Algorithm
  parameters, 228
  support, 225
Spoofing
  hello packets (configuration BPDUs), bridging, 226
  Novell IPX watchdog packets, 205
  Novell IPX, enabling, 209
  Novell SPX keep-alive packets, 206
SPX, see Novell IPX routing, 205
Standard product parts, 23
Stateful filter, 175
  description, 17, 167
  example, 183
Stateful pass filters, 175
Static
  backup routes, configuring (IPX), 220
  Forwarding Table examples, bridging, 231
  Host routes, configuring, 200
  Mapping, NAT, 193
  Multicast Destination Forwarding Table, bridging, 229
  routes
    configuring (IP), 200
    configuring (IPX), 220
    configuring in Intel Device View, 67
    IP, 154
    Novell IPX, 203
    support, 20
  routes and services Example, 223
  services, configuring (IPX), 220
  Source Forwarding Table, bridging, 230
  Type Forwarding Table, bridging, 230
  Unicast Destination Forwarding Table, bridging, 229
Static filters
  description, 17, 167
Statutory notices & warnings, xi
Supported connections, 331
Susceptibility approval, xvii, 318
SVC parameters
  X.25 link, 121
Switched Virtual Circuits (SVCs), X.25, 118
SYN flood protection
  configuring, 173
  description, 17, 172
Syslog server, configuring Log system, 256
System
  Log, see Log System
  Parameters (name, location and contact), 96
System Window, 51
  color-coding of messages, 52
  field descriptions, 52

T

T1
channel allocation, 100
channel speed, 100
description, 99
framing format, 100
line coding, 100
line speed, 100
Taiwan Declaration, xvii
TCP Flags, 177
TCP/IP, see IP routing
Technical Specifications, 317
Telecommunications approvals, xvii, 318
Telnet
access to the router, 92
enabling access to Local Management
enabling Telnet access, 251
enabling access via WAN links, 161
from Intel Device View, 82
management of the router, see Local Management
to Local Management, 10, 82
to router having a default IP address, 83
Temperature specifications, 318
terminal parameters, 31
TFTP
access rights, 248
Advanced Setup management configuration, 247
configuration, 10
enabling access via WAN links, 161
password, 73, 248
Time and Date in the router, 72
Timer Profiles, 149
configuring on a link, 149, 150
setting up, 150
Timing Mode, CSU/DSU, 102
Trap, 249
destinations, 72, 253
Window, 50
Triggered RIP
description, 18, 154
parameter, 158
Troubleshooting, 281
console port, 288
CSU/DSU, 290
duplicate bridged frames, 297
equipment will not boot via a WAN link, 294
general procedure, 282
IP routing will not forward data, 293
IPX routing will not forward data, 296
IPX WAN link will not start up, 295
long delays in bridging, 298
PPP dial-up modem link, 288
router starting with old configuration, 287
tools, 281
typical problems, 287
unable to bridge IP data, 298
unable to bridge IPX data, 297
using Intel Device View, 281
using the LEDs, 281
WAN link will not start up, 291
TTL Threshold
IP Multicast routing, 161
IP Multicast Tunnel, 164
Tunnels
Internet Tunnel, 16
IP Multicast, see IP Multicast Tunneling
Type
(packet type) Forwarding Table, bridging, 230
20 Broadcasts, IPX routing, 209
Typical Problems that could be encountered, 287

U

Unicast Destination Forwarding Table,

bridging, 229
Use of shielded cables, xi

V

V.11 (X.21/V.11) DTE Port Cable, 24, 325
V.24 DTE Port Cable, 24
V.35 DTE Port Cable, 24, 322
V.36 DTE Port Cable, 24, 323
Value-added services, 257
Virtual Circuit parameter
  X.25 link, 121
Virtual Private Networks, see Internet Tunnel

W

WAN
  Bridging, see bridging
  cables, 24
WAN bridging, Frame Relay, 113
WAN link
  adding
    bridging to, 227
    IP routing to, 157
    IPX routing to, 207
  as backup for another link or port, 147
  configuring
    bridging, 225
    IP filtering, 174
    IP routing on, 153
    IPX data filtering, 216
    IPX RIP and SAP filtering, 211
    Novell IPX routing on, 203
  daily activity limit facility, 149
  Frame Relay, 109
  Internet Tunnel, 131
  IPX WAN link will not start up, troubleshooting, 295
  PPP leased line, 103
  remote equipment will not boot, troubleshooting, 294
  will not start up, troubleshooting, 291
  X.25, 118
WAN port
  cables, 24
  configuring using Intel Device View, 60
  connecting, 27
  description, 4
  LEDs, 6
  port specifications, 320
WAN protocol, Novell IPX, 204
WAN services
  specifications, 334
Warnings, 23
Watchdog (Novell IPX)
  packets, 204
  spoofing, 205
Windows Internet Name Service server, see WINS server
WINS server, 65, 244

X

X.25
  addressing parameters, X.31 link, 121
  configuration overview, 119
  configuring for port, 119
  configuring link, 120
  data compression, 13
  data security over using Internet Tunnels, 143
  Default Packet Size, 120
  description and implementation, 13
  Encapsulation Type, 122
  Flow Control, 119
  Highest 2-way Channel, 119
  Lowest 2-way channel, 119
  Permanent Virtual Circuits (PVCs), 118
  Reverse Charges, 13
  RPOA, 122
  services and links configuration, 118
  specifications, 336
  support, 118
  Switched Virtual Circuits (SVCs), 118
X.25 link
  addressing parameters, 121
  Data Compression, 121
  Virtual Circuit parameter, 121
  Window Size, PVC, 121

Automated Support

You can reach Intel® automated support services 24 hours a day, every day at no charge. The services contain the most up-to-date information about Intel products. You can access installation instructions, troubleshooting information, and general product information.

World Wide Web & Internet FTP **Access Intel's World Wide Web page or download information using anonymous FTP.**	
How to Access:	WWW ***Customer Support: http://support.intel.com*** ***News: news://cs.intel.com*** FTP ***Host: download.intel.com***

Customer Support Technicians

Free support for 90 days: You can speak with our technical support professionals free of charge for 90 days after your initial call.

North America only: (916) 377-7000

Other support services: You can purchase a range of support services, including 24 hour support, per incident support, on-site service, and software and hardware maintenance agreements. For details about the Intel Support Service options, go to our Web site at http://support.intel.com/services and choose your geography.

Worldwide access: Intel has technical support centers worldwide. Many of the centers are staffed by technicians who speak the local languages. Go to our Web site at http://www.intel.com/intel/contact to find the Intel support center for your geography.

Country	Number	Language
France	+33 (0) 1 41 91 85 29	French
Germany	+49 (0) 69 9509 6099	German
Italy	+39 (0) 2 696 33276	Italian
UK	+44 (0) 870 607 2439	English

If you don't have access to automated services, contact your local dealer or distributor. Or call +1-916-377-7000 from 07:00 to 17:00 Monday through Friday, U.S. Pacific Time.